Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: JUL 2 4 2019

File No.:
RDIMS No.: 3081739

MEMORANDUM FOR THE MINISTER

FIVE COUNTRY MINISTERIAL MEETING

(Information only)

OVERVIEW NOTE

SUMMARY

You will attend the Five Country Ministerial (FCM) meeting in London, United Kingdom, July 29-30. The U.K. has proposed the following topics to be discussed at the FCM:

1. Cyber Threats (including 5G);
2. Emerging Technologies (Internet of Things and Drones);
3. Borders and Immigration;
4. Countering Foreign Interference;
5. Online Harms (Child Sexual Exploitation and Abuse, and Terrorism and Violent Extremism Online and Offline);
6. Encryption; and,
7. Foreign Terrorist Fighters.

This year's FCM will continue the tradition of holding a joint meeting with the Quintet (i.e. the Attorneys General of the Five Eyes), which will take place on the afternoon of Day 2, July 30. Topics 5-7 in the above list will be discussed in the joint FCM-Quintet format. As you are aware, Minister Lametti will not be attending this year's Quintet; therefore, Associate Deputy Minister of Justice François Daigle will instead represent the Department of Justice. Minister Hussen will lead the Immigration, Refugees, and Citizenship Canada delegation.

As host of the FCM 2019, the U.K. Home Secretary has chosen "Emerging Threats" as the overarching theme for this year's meeting. This overarching theme is intended to capture the Five Eyes' collective focus on both present and future national security risks from hostile states, new technologies, and illicit use of the Internet. Notably, a number of these themes have also been similarly discussed in other international fora in which you participate such as the G7. Finally, there will be a roundtable discussion between security and immigration ministers and representatives of digital industry to discuss child sexual exploitation and abuse.

Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The FCM will take place at a unique time in U.K. politics, with Boris Johnson having just been announced as the successor to Prime Minister Theresa May. Moreover, this change in leadership has resulted in a cabinet shuffle and therefore a change of the Home Secretary. Despite these changes, the U.K. has assured Five Eyes partners that the FCM and Quintet will go ahead as planned.

The other FCM Ministers in attendance will be:

- The Right Honourable Priti Patel, Secretary of State for the Home Department, U.K.
- The Honourable Peter Dutton, Minister for Home Affairs, Australia
- The Honourable Andrew Little, Minister for Justice, Courts, and Treaty of Waitangi Negotiations, New Zealand
- The Honorable Kevin McAleenan, Acting Secretary of Homeland Security, U.S.

Bilateral meetings have been scheduled with Secretary Patel, Minister Dutton, Minister Little, and Secretary McAleenan. A bilateral meeting has also been scheduled with United States Attorney General William Barr, who will be in London to participate in the Quintet. You will be accompanied by staff from your office and officials from the Department for each of your bilateral meetings. Canadian High Commissioner to the U.K. Janice Charette may also join you as appropriate.

Enclosed are the following materials for your visit:

- FCM agenda (**Foldout at the back of this binder**);
- Itinerary for your visit to the U.K. (**TAB B**);
- Canadian Delegation information (**TAB C**);
- Scenario notes (prepared by PS officials) and background position papers (prepared by the lead Five Eyes partner for that topic) for each session, along with relevant annexes (**TABS D, E, and 1-11**);
- Materials to support your bilateral meetings (**TABS F-J**); and,
- Supplementary reading materials related to FCM topics for further background reading (**TAB K**).

MEETING FORMAT

The FCM will take place at Carlton House Terrace, a short distance from your hotel. The meeting room will be cleared to SECRET. Furthermore, there will be two Public Safety Canada officials in the meeting room to support you during the sessions.

As the host, it is expected that the U.K. Home Secretary will formally chair each session at the FCM. Following his/her opening remarks at each session, he/she will turn to the minister representing the lead country for a particular topic to help frame the discussion. Following this, the floor will then open for ministerial discussion. You will co-lead the sessions on Countering Foreign Interference (with Australia) and on Online Harms/Terrorism and Violent Extremism Online and Offline (with New Zealand), both scheduled on Day 2.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

STRATEGIC OBJECTIVES

The strategic objectives for this meeting are:

- [redacted]

BACKGROUND

The FCM is an annual meeting of the security and immigration ministers of the Five Eyes partners: Australia, Canada, New Zealand, the United Kingdom, and the United States. The FCM was created as the ministerial forum to discuss policies, operational approaches, and legal measures on a range of national security and public safety issues facing the Five Eyes partners. The first meeting took place in Monterey, California, in 2013; subsequent meetings took place in London (2015), Washington, D.C. (2016), Ottawa (2017), and Gold Coast, Australia (2018). Your participation in the FCM 2019 will be the sixth time that Canada has participated in the FCM. [redacted]

Should you require additional information, please do not hesitate to contact myself or Monik Beauregard, Senior Assistant Deputy Minister, National Cyber and Security Branch at 613-990-4976.

Gina Wilson

Prepared by: Justin Chan

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FIVE COUNTRY MINISTERIAL



Emerging Threats London 2019

Minister Goodale

s.13(1)(a)
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL

Emerging Threats
London 2019

AGENDA

29-30 July 2019

DAY 1

Time	Item	Lead
0815 - 0830	**Welcome and Administration** *Home Secretary welcome, and theme introduction*	UK
0830 - 0915	**Ministerial statements on priorities** *Home Secretary to invite other Ministers to introduce short 'priority statements'*	ALL
0915 - 1000	**Threat Assessments** [redacted]	UK
1000 - 1015	**MORNING TEA**	
1015 - 1230	**Cyber Threats** *Current threats and response,* [redacted] *Cyber and 5G* *Session outcomes*	UK US/UK
1230 - 1330	**LUNCH** (FCM Ministers +1) **OFFICIAL PHOTOGRAPHS** (FCM Ministers Only)	
1330 - 1515	**Emerging Technologies** *'Internet of Things'* *Drones* *Session outcomes*	AUS UK
1515 - 1530	**AFTERNOON TEA**	
1530 - 1700	**Borders & Immigration** [redacted] *Session outcomes*	AUS AUS/UK
1700 - 1825	**BILATERALS**	
1830 - 1900	**TRANSFER**	
1900	**DRINKS RECEPTION (All) at White Tower, Tower of London**	
2000	**DINNER (FCM Ministers +2) in Medival Palace followed by Ceremony of the Keys** **Ministerial Discussion: Social Integration**	
2000 - 2100	**DINNER (Other delegates) at White Tower, Tower of London**	

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

AGENDA
29-30 July 2019

DAY 2

Time	Item	Lead
0900 - 1100	**Industry Roundtable on CSEA** *Attended by Microsoft, Twitter, Facebook, Google, Snap & Roblox*	ALL
1100 - 1115	**MORNING TEA**	
1115 - 1200	**Countering Foreign Interference** *Election security and strengthening democracy* *Session outcomes*	AUS/CAN
1200 - 1230	**Draft FCM Communiqué**	ALL
1230 - 1315	**JOINT FCM/QUINTET LUNCH** (Ministers + 1) **OFFICIAL PHOTOGRAPHS** (FCM & Quintet Ministers Only)	

s.13(1)(a)
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

AGENDA
29-30 July 2019

JOINT FCM/QUINTET SESSIONS

Time	Item	Lead
1315 – 1500	**Online Harms** *Countering child sexual exploitation and abuse* *Preventing terrorist use of the internet and countering extremism* *Session outcomes*	 UK CAN/NZ
1500 - 1515	**AFTERNOON TEA**	
1515 - 1615	**Encryption** *Session outcomes*	UK
1615 - 1715	**Foreign Terrorist Fighters** *Battlefield evidence,* [redacted] *and PNR/UNSCR 2396* *Session outcomes*	 UK/US
1715 - 1730	**Finalise Joint Communiqué**	ALL
1730 - 1800	**BREAK / BILATERALS**	
1815 - 1845	**PRESS CONFERENCE** (FCM Ministers only)	
1850	**TRANSFER**	
1900	**JOINT FCM/QUINTET DRINKS RECEPTION (All) at Gray's Inn**	

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Session	Policy Lead Coordinates
[redacted]	• PS: **Alex Corbeil** | alexander.corbeil@canada.ca | 613-998-8520
	• [redacted]
	• PS: [redacted]
	• PS: **Sarah McIntosh**| sarah.mcintosh@canada.ca | 613-990-7050 • PS: **Kelly-Anne Gibson** | kelly-anne.gibson2@canada.ca | 613-990-9608
	• PS: **Fadi Balesh** | fadi.balesh2@canada.ca | 613-990-1699 • PS: **Srishti Hukku** | srishti.hukku@canada.ca |613-949-0361
Cyber Threats: Current Threats and Response	• PS: **Sarah McIntosh**| sarah.mcintosh@canada.ca | 613-990-7050 • PS: **Kelly-Anne Gibson** | kelly-anne.gibson2@canada.ca | 613-990-9608
Cyber Threats: Cyber and 5G	• PS: **Sarah McIntosh** | sarah.mcintosh@canada.ca | 613-990-7050 • PS: **Kelly-Anne Gibson** | kelly-anne.gibson2@canada.ca | 613-990-9608
Emerging Technologies: Internet of Things	• PS: **Sarah McIntosh** | sarah.mcintosh@canada.ca | 613-990-7050 • PS: **Kelly-Anne Gibson** | kelly-anne.gibson2@canada.ca | 613-990-9608
Emerging Technologies: Drones	• **Jon-Paul Hanley** | jon-paul.hanley@tc.gc.ca • **Justin Jedlinski** | justin.jedlinski@tc.gc.ca • **Phillip Spear** | phillip.spear@tc.gc.ca
Borders and Immigration: [redacted]	• CBSA: **Erin Murray** | erinm.murray@cbsa-asfc.gc.ca | 613-314-3903 • CBSA: **Mary-Teresa Glynn** | MaryTeresa.Glynn@international.gc.ca | +44(0)20 7004 6220
Borders and Immigration: [redacted]	• CBSA: **Erin Murray** | erinm.murray@cbsa-asfc.gc.ca | 613-314-3903 • CBSA: **Mary-Teresa Glynn** (UK Liaison Officer) | MaryTeresa.Glynn@international.gc.ca | +44(0)20 7004 6220
Dinner Discussion: Social Integration, Inclusion and Identity	• PS: **Catherine Giguere** | catherine.giguere@canada.ca | 613-949-1791 • PS: **Michael King** | michael.king5@canada.ca | 613-991-4897
Industry Roundtable	• PS: **Mathilde Briere-Audet** | mathilde.briere-audet@canada.ca | 613-949-9075 • PS: **Tara Gray** | tara.gray@canada.ca | 613-998-8034
Countering Foreign Interference:	• PS: [redacted]

s.13(1)(a)
s.15(1) - Int'l
s.15(1) - Subv

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Online Harms: Child Sexual Exploitation and Abuse	• PS: **Mathilde Briere-Audet** | mathilde.briere-audet@canada.ca | 613-949-9075 • PS: **Tara Gray** | tara.gray@canada.ca | 613-998-8034
Online Harms; Violent Extremism and Terrorist Use of the Internet	• PS: **Alex Corbeil** | alexander.corbeil@canada.ca | 613-998-8520
Encryption	• PS: [redacted] • PS: **Sophie Beecher** | sophie.beecher@canada.ca | 613-949-3184 • PS: [redacted]
Foreign Terrorist Fighters	• PS: [redacted] • PS: **Matthew Mayer** | matthew.mayer@canada.ca | 613-999-9999

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FIVE COUNTRY MINISTERIAL (FCM)
JULY 29-30, 2019

Table of Contents

OVERVIEW NOTE AND 2018 FCM PROGRESS REPORT TAB A

BILATERAL SCHEDULE AND DRAFT ITINERARY TAB B

CANADIAN DELEGATION CONTACT INFORMATION AND LOGISTICS NOTE TAB C

FCM SESSIONS

Ministerial Statements on Priorities TAB D

Threat Assessments TAB E

Session 1: Cyber Threats TAB 1

Session 2: Emerging Technologies TAB 2

Session 3: Borders and Immigration TAB 3

Session 4: Dinner Discussion: Social Integration, Inclusion, and Identity TAB 4

Session 5: Industry Roundtable on Child Sexual Exploitation and Abuse TAB 5

Session 6: Countering Foreign Interference TAB 6

Session 7: Draft FCM Communiqué TAB 7

JOINT FCM-QUINTET SESSIONS

Session 8: Online Harms TAB 8

Session 9: Encryption TAB 9

Session 10: Foreign Terrorist Fighters TAB 10

Session 11: Draft Joint FCM-Quintet Communiqué TAB 11

BILATERAL MEETINGS

William Barr, Attorney General, United States TAB F
Scenario note and biography

David Pekoske, Acting Deputy Secretary of Homeland Security, United States TAB G
Scenario note and biography

s.15(1) - Int'l
s.15(1) - Subv
s.15(1)(d)(ii)
s.16(1)(a)(iii)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Priti Patel, Home Secretary, United Kingdom — TAB H
Scenario note and biography

Andrew Little, Minister for Justice, Courts and Treaty of Waitangi Negotiations, New Zealand — TAB I
Scenario note and biography

Peter Dutton, Minister of Home Affairs, Australia — TAB J
Scenario note and biography

SUPPLEMENTARY INFORMATION — TAB K

Bloomberg: Trump Says Huawei 5G Debate Poses 'No Problem to U.S.-U.K. Ties

U.K. Online Harms White Paper

[redacted]

C3P Report: Child Sexual Abuse Images on the Internet – Summary

C3P Report: International Survivors – Summary

Thorn Report: Role of Technology in Minor Sex Trafficking – Summary

[redacted]

Facebook Blog Post: Standing Against Hate

NY Times: YouTube's Product Chief on Radicalization and Algorithmic Rabbit Holes

VOX: How the Christchurch Shooter Used Memes to Spread Hate

NY Times: Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger

FCM AGENDA — BACK FOLDOUT

QUINTET AGENDA — BACK SLEEVE

Page 12

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 15(1) - Subv

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: JUL 2 4 2019

File No.: PS-028671

RDIMS No.: 3081739

MEMORANDUM FOR THE MINISTER

FIVE COUNTRY MINISTERIAL MEETING

(Information only)

OVERVIEW NOTE

SUMMARY

You will attend the Five Country Ministerial (FCM) meeting in London, United Kingdom, July 29-30. The U.K. has proposed the following topics to be discussed at the FCM:

1. Cyber Threats (including 5G);
2. Emerging Technologies (Internet of Things and Drones);
3. Borders and Immigration;
4. Countering Foreign Interference;
5. Online Harms (Child Sexual Exploitation and Abuse, and Terrorism and Violent Extremism Online and Offline);
6. Encryption; and,
7. Foreign Terrorist Fighters.

This year's FCM will continue the tradition of holding a joint meeting with the Quintet (i.e. the Attorneys General of the Five Eyes), which will take place on the afternoon of Day 2, July 30. Topics 5-7 in the above list will be discussed in the joint FCM-Quintet format. As you are aware, Minister Lametti will not be attending this year's Quintet; therefore, Associate Deputy Minister of Justice François Daigle will instead represent the Department of Justice. Minister Hussen will lead the Immigration, Refugees, and Citizenship Canada delegation.

As host of the FCM 2019, the U.K. Home Secretary has chosen "Emerging Threats" as the overarching theme for this year's meeting. This overarching theme is intended to capture the Five Eyes' collective focus on both present and future national security risks from hostile states, new technologies, and illicit use of the Internet. Notably, a number of these themes have also been similarly discussed in other international fora in which you participate such as the G7. Finally, there will be a roundtable discussion between security and immigration ministers and representatives of digital industry to discuss child sexual exploitation and abuse.

Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The FCM will take place at a unique time in U.K. politics, with Boris Johnson having just been announced as the successor to Prime Minister Theresa May. Moreover, this change in leadership has resulted in a cabinet shuffle and therefore a change of the Home Secretary. Despite these changes, the U.K. has assured Five Eyes partners that the FCM and Quintet will go ahead as planned.

The other FCM Ministers in attendance will be:

- The Right Honourable Priti Patel, Secretary of State for the Home Department, U.K.
- The Honourable Peter Dutton, Minister for Home Affairs, Australia
- The Honourable Andrew Little, Minister for Justice, Courts, and Treaty of Waitangi Negotiations, New Zealand
- The Honorable Kevin McAleenan, Acting Secretary of Homeland Security, U.S.

Bilateral meetings have been scheduled with Secretary Patel, Minister Dutton, Minister Little, and Secretary McAleenan. A bilateral meeting has also been scheduled with United States Attorney General William Barr, who will be in London to participate in the Quintet. You will be accompanied by staff from your office and officials from the Department for each of your bilateral meetings. Canadian High Commissioner to the U.K. Janice Charette may also join you as appropriate.

Enclosed are the following materials for your visit:

- FCM agenda (**Foldout at the back of this binder**);
- Itinerary for your visit to the U.K. (**TAB B**);
- Canadian Delegation information (**TAB C**);
- Scenario notes (prepared by PS officials) and background position papers (prepared by the lead Five Eyes partner for that topic) for each session, along with relevant annexes (**TABS D, E, and 1-11**);
- Materials to support your bilateral meetings (**TABS F-J**); and,
- Supplementary reading materials related to FCM topics for further background reading (**TAB K**).

MEETING FORMAT

The FCM will take place at Carlton House Terrace, a short distance from your hotel. The meeting room will be cleared to SECRET. Furthermore, there will be two Public Safety Canada officials in the meeting room to support you during the sessions.

As the host, it is expected that the U.K. Home Secretary will formally chair each session at the FCM. Following his/her opening remarks at each session, he/she will turn to the minister representing the lead country for a particular topic to help frame the discussion. Following this, the floor will then open for ministerial discussion. You will co-lead the sessions on Countering Foreign Interference (with Australia) and on Online Harms/Terrorism and Violent Extremism Online and Offline (with New Zealand), both scheduled on Day 2.

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

STRATEGIC OBJECTIVES

The strategic objectives for this meeting are:

- [redacted]

BACKGROUND

The FCM is an annual meeting of the security and immigration ministers of the Five Eyes partners: Australia, Canada, New Zealand, the United Kingdom, and the United States. The FCM was created as the ministerial forum to discuss policies, operational approaches, and legal measures on a range of national security and public safety issues facing the Five Eyes partners. The first meeting took place in Monterey, California, in 2013; subsequent meetings took place in London (2015), Washington, D.C. (2016), Ottawa (2017), and Gold Coast, Australia (2018). Your participation in the FCM 2019 will be the sixth time that Canada has participated in the FCM. [redacted]

Should you require additional information, please do not hesitate to contact myself or Monik Beauregard, Senior Assistant Deputy Minister, National Cyber and Security Branch at 613-990-4976.

Gina Wilson

Prepared by: Justin Chan

Pages 16 to / à 19

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Page 20

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 15(1) - Int'l, 15(1) - Subv

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1) - Subv

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

UNCLASSIFIED
Updated 07/26/2019, 12:45

PARTICIPATION OF THE MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS, THE HONOURABLE RALPH GOODALE, TO THE FIVE COUNTRY MINISTERIAL MEETING LONDON, UNITED KINGDOM JULY 27-31, 2019

ITINERARY

DAY 1 – SATURDAY JULY 27, REGINA

[redacted]

DAY 2 – SUNDAY JULY 28, LONDON, UK

(Time difference from Ottawa +5 hours)

[redacted]

RDIMS: 3066491

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

15:00-15:30 **Pre-briefing for bilateral meeting with Attorney General W. Barr (US)**
Location: [redacted]

Participants: Minister Goodale
D. Hurl
François Daigle, Associate Deputy Minister of Justice
Elizabeth Eid, Assistant Deputy Minister for Public Safety, Defence and Immigration Portfolio, Justice Canada
M. Beauregard
J. Wherrett
O. Cullen

15:30-16:00 **Bilateral meeting with Attorney General William Barr, United States**
Location: [redacted]
Participants: Minister Goodale
F. Daigle
D. Hurl
E. Eid
J. Wherrett

[redacted]

16:15-17:30 **Briefing with the Public Safety Delegation**
Location: Canada House
Participants: PS whole delegation.
Note: HC Charette to join around 5 pm.

17:30-19:30 **Informal Drinks Reception**
Note: hosted by Canada's High Commissioner, Janice Charette
Location: Canada House
Participants: All - optional

After 19:30 Personal time

s.13(1)(a)
s.15(1) - Int'l
s.15(1) - Subv

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

DAY 3 – MONDAY, JULY 29, LONDON

[redacted]

8:15-8:30 **Welcome and Administration**
Home Secretary welcome and theme introduction
Location: The Council Room (no electronics), Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: D. Hurl

8:30-9:15 **Ministerial Statements on Priorities**
Home Secretary to invite other Ministers to introduce short 'priority statements'
Note: Each minister is provided five minutes.
Location: The Council Room (no electronics), Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: D. Hurl

9:15-10:00 **Threat Assessment** (UK lead)
[redacted]
Note: Each minister is provided five minutes for reaction to the presentation.
Location: The Council Room (no electronics), Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: D. Hurl

10:00-10:15 Morning tea
Location: The Music Room, Carlton House Terrace
Participants: Entire delegation

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

10:15-12:30 **Cyber Threats**

- *Current threats and response,* [redacted] *(UK lead)*
- *Cyber and 5G (US/UK lead)*
- *Session outcomes*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: D. Hurl

12:30-13:30 **Lunch and Official Photographs**
Location: The Music Room, Carlton House Terrace
Participant: Minister Goodale
O. Cullen

13:30-15:15 **Emerging Technologies**

- *'Internet of Things' (Aus lead)*
- *Drones (UK lead)*
- *Session outcomes*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: O. Cullen

15:15-15:30 Afternoon Tea
Location: The Music Room, Carlton House Terrace
Participants: All

15:30-17:00 **Borders & Immigration**

[redacted]

- *Session outcomes (Minister Hussen to lead on Canada's reaction)*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: O. Cullen

17:00-17:25 **Trilateral meeting with Minister Hussen and, David Pekoske, Acting Deputy Secretary of Homeland Security, United States**
Location: The Music Room, Secret-cleared, Carlton House Terrace
Participants: Minister Goodale
D. Hurl
M. Beauregard
J. Wherrett
O. Cullen

17:25-17:30 Break

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

17:30-17:55 **Bilateral meeting with Priti Patel, Home Secretary, United Kingdom**
Note: A gift exchange is to take place.
Location: The Council Room, Secret-cleared, Carlton House Terrace
Participants: Minister Goodale
High Commissioner Charette
D. Hurl
M. Beauregard
J. Wherrett

17:55-18:00 Break

18:00-18:25 **Bilateral meeting with Andrew Little, Minister for Justice, Courts and Treaty of Waitangi Negotiations of New Zealand**
Location: The Council Room, Secret-cleared, Carlton House Terrace
Participants: Minister Goodale
F. Daigle
D. Hurl
E. Eid
J. Wherrett

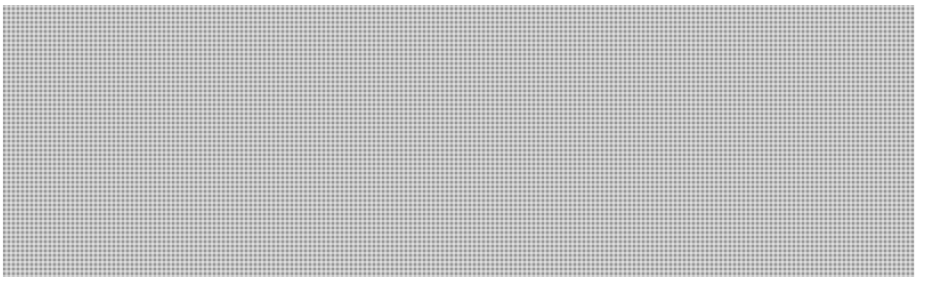
[redacted]

19:00-20:00 **Drinks Reception**
Location: Tower of London
Participants: All

20:00-21:30 **FCM Ministerial Dinner**
Discussion on Social Integration (Aus lead)
Location: Medieval Palace, Tower of London
Participants: Minister Goodale
D. Hurl
J. Wherrett
Note: Other delegates to be provided dinner at White Tower, Tower of London.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

21:30-22:05 **Ceremony of the Keys**
Location: Tower of London
Participants: Minister Goodale
D. Hurl
J. Wherrett



s.15(1) - Subv

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

DAY 4 – TUESDAY, JULY 30, LONDON

7:40-8:40 **Breakfast briefing with the Public Safety delegation**
Location: Adam Suite (not secret-cleared), first floor, Amba Charing Cross Hotel
Participants: PS whole delegation

8:40 [redacted]

9:00-11:00 **Industry Roundtable on Countering Online Child Sexual Exploitation and Abuse (SCEA)** (All lead)
Attended by:
1. *Facebook – Antigone Davis*
2. *Google – Leslie Miller*
3. *Microsoft – Jacqueline Beauchere*
4. *Snap – Jennifer Park-Stout*
5. *Twitter – Katy Minshall*
6. *Roblox – Remy Malan*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: T. Bhupsingh
Back row: D. Hurl / J. Wherrett

11:00-11:15 Morning tea
Location: The Music Room, Carlton House Terrace
Participants: All

11:15-12:00 **Countering Foreign Interference and Communiqué**
- *Election Security and Strengthening Democracy (Aus/Can lead)*
- *Session outcomes*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: O. Cullen

12:00-12:30 **Finalize FCM Communiqué** (All lead)
Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: O. Cullen

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

12:30-13:15 **Joint FCM/Quintet Lunch and Official Photographs**
Location: The Music Room, Carlton House Terrace
Participants: Minister Goodale
D. Hurl

13:15-15:00 **Online Harms (Joint FCM/Quintet)**
- *Countering Child Sexual Exploitation and Abuse (UK lead)*
- *Preventing and countering terrorism and violent extremism (Can/NZ lead)*
- *Session outcomes*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: J. Wherrett
Back row: T. Bhupsingh

15:00-15:15 Afternoon tea
Location: The Music Room, Carlton House Terrace
Participants: All

15:15-16:15 **Encryption** (UK Lead)
- *Online safety*
- *Session outcomes*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: D. Hurl

16:15-17:15 **Foreign Terrorist Fighters**
- *Battlefield evidence,* [redacted] *and PNR/UNSCR 2396 (UK/US lead)*
- *Session outcomes*

Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: D. Hurl

17:15-17:30 **Finalise Joint Communiqué (FCM/Quintet)** (All lead)
Location: The Council Room, Carlton House Terrace
Participants: Minister Goodale
At the table: M. Beauregard
Back row: D. Hurl

s.15(1) - Subv

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

17:30-18:00 **Bilateral meeting with Peter Dutton, Minister of Home Affairs, Australia**
Location: The Council Room, Secret-cleared, Carlton House Terrace
Participants: Minister Goodale
D. Hurl
M. Beauregard
J. Wherrett
Mary-Theresa Glynn (for note taking)

18:15-18:45 **Press Conference** (FCM Ministers only)
Note: The UK Home Secretary will deliver opening remarks, and then open for a Q+A session with participants. Opening remarks not required.
Location: The Library Room, Carlton House Terrace
Participant: Minister Goodale

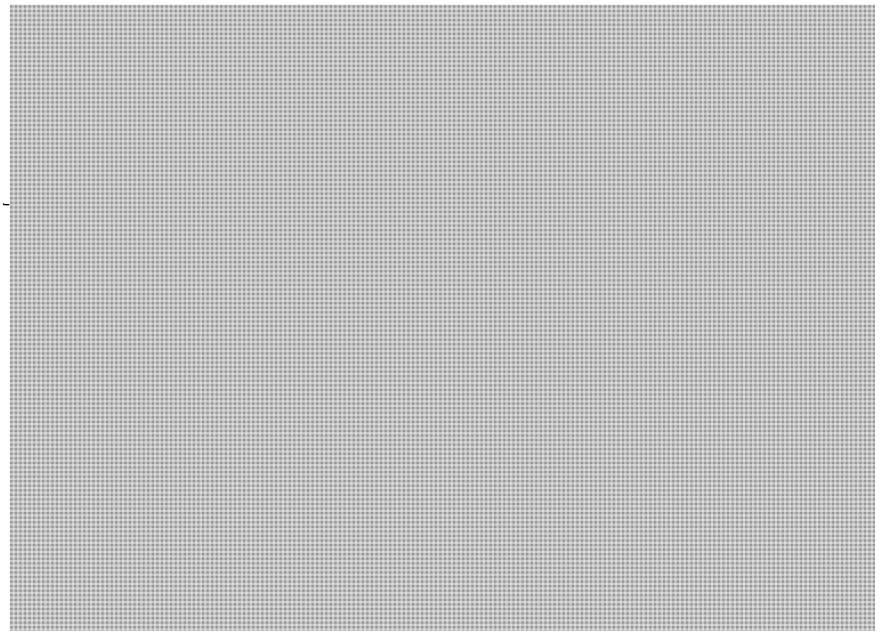
[redacted]

19:00-20:00 **Drinks Reception**
Location: Honourable Society of Gray's Inn
Participants: All
Note: 'Bowl food' will be provided to all.

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

DAY 5 – WEDNESDAY, JULY 31, LONDON-REGINA



END OF PROGRAM

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada Delegation Contact Information

Name	Titles	Cell Phone Number	Email
Minister Goodale	Minister of Public Safety, Head of Delegation		Ralph.Goodale@parl.gc.ca
David Hurl	Office of the Minister	613-769-8342	David.Hurl@canada.ca
Olivier Cullen	Office of the Minister	343-998-1482	Olivier.Cullen@canada.ca
Monik Beauregard	Senior Assistant Deputy Minister, National and Cyber Security Branch	PIN:	Monik.Beauregard@canada.ca
Jill Wherrett	Assistant Deputy Minister, Portfolio Affairs and Communications	PIN:	Jill.Wherrett@canada.ca
Trevor Bhupsingh	Director-General, Law Enforcement and Border Strategies	613-769-3042 PIN:	Trevor.Bhupsingh@canada.ca
	Senior Director, National Security Policy		@canada.ca
Adam Green	Manager, Policy Development, National Security Policy	613-271-5199	Adam.Green@canada.ca
Mike Williams	First Secretary (Political), High Commission of Canada	+044(0) 77 7847 2985	Mike.Williams@international.gc.ca
Mary-Teresa Glynn	CBSA Liaison Officer, Canadian Border Services Agency	+044(0) 78 2538 9300	MaryTeresa.Glynn@international.gc.ca

UK Home Office Delegation Liaison Officer (DLO) Assigned to Public Safety Canada

Andy Black	UK DLO		

Pages 32 to / à 37

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l, 15(1) - Subv

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

ABOUT LONDON

Things to do

Westminster Abbey (right)



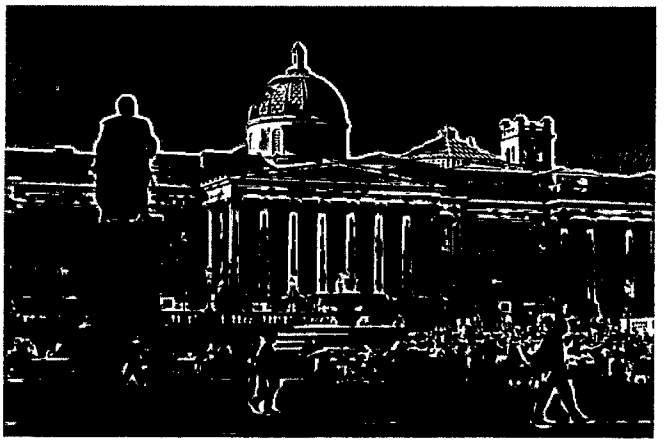
Located in the heart of Westminster and a short walk away from the Houses of Parliament, Big Ben and the London Eye, the Abbey welcomes over one million visitors each year who want to explore this wonderful 700-year-old building - the coronation church of England.

Tate Modern

Sitting grandly on the banks of the Thames is Tate Modern, Britain's national museum of modern and contemporary art. Its unique shape is due to it previously being a power station. The gallery's restaurants offer fabulous views across the city.

British Museum

The world-famous British Museum exhibits the works of man from prehistoric to modern times, from around the world. Highlights include the Rosetta Stone, the Parthenon sculptures and the mummies in the Ancient Egypt collection.



National Gallery (left)

The crowning glory of Trafalgar Square, London's National Gallery is a vast space filled with western European paintings from the 13th to the 19th centuries. Find works by masters such as Van Gogh, da Vinci, Botticelli, Constable, Renoir, Titian and Stubbs.

Victoria and Albert Museum

The V&A celebrates art and design with 3,000 years' worth of artefacts from around the world: furniture, paintings, sculptures, metalwork, and textiles.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Bars, Pubs and Restaurants

There are many bars, pubs and restaurants located in the vicinity of Westminster, catering to a wide variety of tastes.

The Admiralty

The Admiralty is located right on the southern edge of Trafalgar Square making it officially London's most central pub. It backs onto St James's Park and Admiralty Arch, from which the pub takes its name.

The Westminster Arms

The Westminster Arms is in the heart of political London, a stone's throw from the Houses of Parliament.

Swan, Shakespeare's Globe

Located at the iconic Shakespeare's Globe, Swan is a bar and restaurant set over two floors, with stunning views of the Thames and St Paul's. Swan is open all day, serving modern British food, cocktails and other drinks.

The Cinnamon Club

The Cinnamon club is a Grade II-listed Victorian building and the high ceiling, book-gallery and crisp napery convey a sense of occasion. Located in Westminster, this restaurant is dedicated to innovative and creative Indian cuisine.

The Rubens at the Palace

Overlooking Buckingham Palace and within easy walking distance of Victoria Station, this historic hotel offers a host of new restaurants and bars. Guests can enjoy live music in the New York Bar, a Royal Afternoon Tea in the Palace Lounge, delicious cuisine in The English Grill and authentic flavours in The Curry Room.

Dukes Bar

One of London's true classic bars, and justly famous for the theatrical presentation of martinis. Planted squarely in St James's, Dukes Bar is an ode to timeless elegance, with old portraits hanging on the walls, emerald velvet armchairs and a wood-panelled bar in the corner.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

MINISTERIAL STATEMENT ON PRIORITIES

Strategic Objectives

- Explain Canada's national security priorities to Five Eyes partners and specific objectives for the Five Country Ministerial meeting.

Key Messages

Your suggested remarks are attached separately.

Background

The U.K. Home Secretary will provide opening remarks and invite Ministers to make a short opening statement on their key national security priorities. You will lead on Canada's statement, followed by Minister Hussen. There are no specific deliverables to agree to during this session.

Drafted: NCSB/NSPD/Justin Chan/Scott Shaw
Consulted:
Approved by: NCSB/Beauregard

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Five Country Ministerial 2019

Ministerial Statement of Priorities

Remarks

for

The Honourable Ralph Goodale

Minister of Public Safety and Emergency Preparedness

Monday, July 29, 2019

London, United Kingdom

Word count for remarks: 751 words (6.25 minutes @ 120wpm)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Introduction

- Fellow Ministers, it is an honour and a pleasure to join you again for the Five Country Ministerial here in London.

- I would like to extend my sincerest personal thanks to the Home Secretary and [his/her] team for organizing this meeting and I look forward to this open and honest discussion.

Canada's Approach to National Security

- The Government of Canada is committed to working in very close partnership with our Five Eyes colleagues, building on a long and established history of cooperation.

- Since our last meeting in Gold Coast, Australia, the Government of Canada has taken robust steps to enhance the security of Canadians:

- The *National Security Act* was recently passed by Parliament and has received royal assent. This represents a major reform to Canada's national security framework and will strengthen security while at the same time enhancing accountability

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

and transparency.

- In December of last year, Canada released a *National Strategy on Countering Radicalization to Violence*, which focuses on three priorities: building the knowledge base on radicalization to violence; addressing radicalization to violence in the online space; and supporting interventions.

- Following the horrific terrorist attack on March 15 2019 on the Muslim community of Christchurch, New Zealand, Canada joined governments and industry leaders from across the globe in adopting the *Christchurch Call to Action* and committing to meeting its goals.

- As part of these commitments, we have announced funding for *Tech Against Terrorism,* which will support smaller tech companies in building their capacities to quickly remove violent extremist and terrorist content.

- We know that the fight against terrorism and violent extremism will take place as much online as it does on our streets and in our communities, and I look forward to our ongoing engagement with

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

digital industry.

- Still in the fight against terrorism, the Government of Canada recently published an update to our *Criminal Code* list of terrorist entities that included, for the first time, two right-wing extremist groups with a presence in Canada.

- Additionally, combatting the phenomenon of terrorist fighters remains a key priority for Canada and our national security agencies. We take all potential threats very seriously and employ the full toolkit of measures to address them

- The security of Canada is also affected by foreign interference. We all continue to be faced with attempts by foreign actors to subvert our democratic institutions and processes and foment polarization. We must remain vigilant in guarding against these threats.

- With Canada's next federal election scheduled to take place in October of this year, we are acutely

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

aware of the magnitude of this issue and proactive measures are being taken.

- I look forward to expanding on these measures further during our discussions.

- Finally, online child sexual exploitation and abuse is one of the most pressing public safety concerns for Canada.

- In March 2019, the Government of Canada announced further investments to better protect children from sexual exploitation online. This funding will support Canada's efforts to raise awareness of this serious issue, reduce the stigma associated with reporting, increase Canada's ability to pursue and prosecute offenders, and work with digital industry to find new ways to combat the sexual exploitation of children online.

- What is more, we remain dedicated to ensuring the security and prosperity of Canadians in the digital age through our new *National Cyber Security Strategy*. Budgets for 2018 and 2019 commit close to $1 billion in support of the *Strategy* and cyber security. This represents the Government of

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Canada's largest investment in cyber security to date.

Conclusion and Invitation to Minister Hussen to speak

- The safety and security of Canadians is the top priority of my Government, and we will continue to take appropriate action to address all threats.

- The Five Eyes partnership remains one of Canada's most important security relationships. We look forward to a robust discussion over the next two days on how we can work together to better ensure the safety and security our citizens.

- At this time, I would like to invite my colleague, the Honourable Minister Ahmed Hussen, Minister of Immigration, Refugees, and Citizenship to say a few words.

- Thank you.

Word Count: 751 words
Time: 6.25 minutes

s.13(1)(a)
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

BRIEFING NOTE FOR THE MINISTER

THREAT ASSESSMENTS

Strategic Objectives

- [redacted]
- [redacted]
- Following the presentation of the assessments, Ministers will be allowed to make interventions for up to five minutes. The below key messages have been provided should you wish to raise any points.

Key Messages

Right-Wing Extremism (RWE)

- The right-wing extremism landscape in Canada is complex, and individuals in this milieu are driven by a range of grievances from across the traditional political spectrum.

- Canada has experienced first-hand the threat posed by individuals and online communities who harbour extreme right-wing views and are promoting or engaging in acts of violence. We have not only witnessed these inspired attacks: we have felt the impact of attackers using low-sophistication tactics, such as vehicle ramming and firearms, to cause harm in pursuit of ideological goals.

- The devastating attacks in Christchurch, New Zealand in March were a stark reminder of the serious impact of violence motivated by extreme ideological views. They also further highlighted how the threat actors use the Internet to advance their objectives by glorifying and sensationalizing acts of violence on a global scale and with an immediate impact.

- Canada continues to explore how to address this evolving threat, and has taken steps in this regard. On June 26th, Canada added two international right-wing extremist groups to its list of terrorist entities. "Blood & Honour" and its armed wing, "Combat 18", have a presence in Canada and

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

are the first right-wing extremist groups to be added to the Canadian *Criminal Code* list.

- [redacted]
- [redacted]

Counter-Terrorism

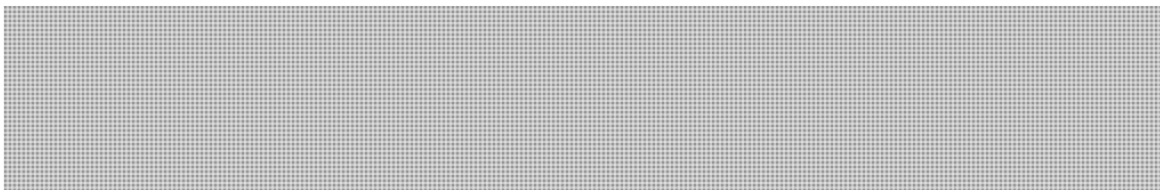
- Despite the destruction of its Caliphate, Daesh will continue to spread its message, attract followers, and encourage its supporters to conduct attacks (including and especially low-sophistication attacks by homegrown extremists).
- [redacted]
- Countries around the world are grappling with how to address returning and potential returning foreign terrorist fighters (FTFs) who have engaged in threat activities abroad.
- [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Foreign Interference

- Activities by hostile states are detrimental to Canada's economic, industrial, military, and technological advantages, necessitating an ongoing understanding of intent and capability. This is particularly important to protect the integrity of Canadian democratic institutions. Canada is not alone in facing this persistent threat.

- 

- The impact, scale, speed, and range of foreign interference has grown as a result of the Internet, social media platforms, and the availability of cheaper and more accessible cyber tools – all with the aim of destabilizing the internal cohesion of other countries, swaying their decision-making, or influencing their political processes.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Foreign threat actors, most notably hostile states and state-sponsored actors, are targeting Canada's democratic institutions and processes. While Canada's electoral system is strong, threat actors have sought to target politicians, political parties, elections, and media outlets in order to manipulate the Canadian public and interfere with Canada's democracy.

- [redacted]

- As our adversaries continue to develop and employ increasingly sophisticated techniques, Canada and our allies must ensure we have the authorities and tools to keep pace. [redacted]

Cyber

- Emerging technologies [redacted] are poised to radically transform the global order. These technologies are revolutionary advancements that will have transformative and disruptive impacts on national security and economic interests.

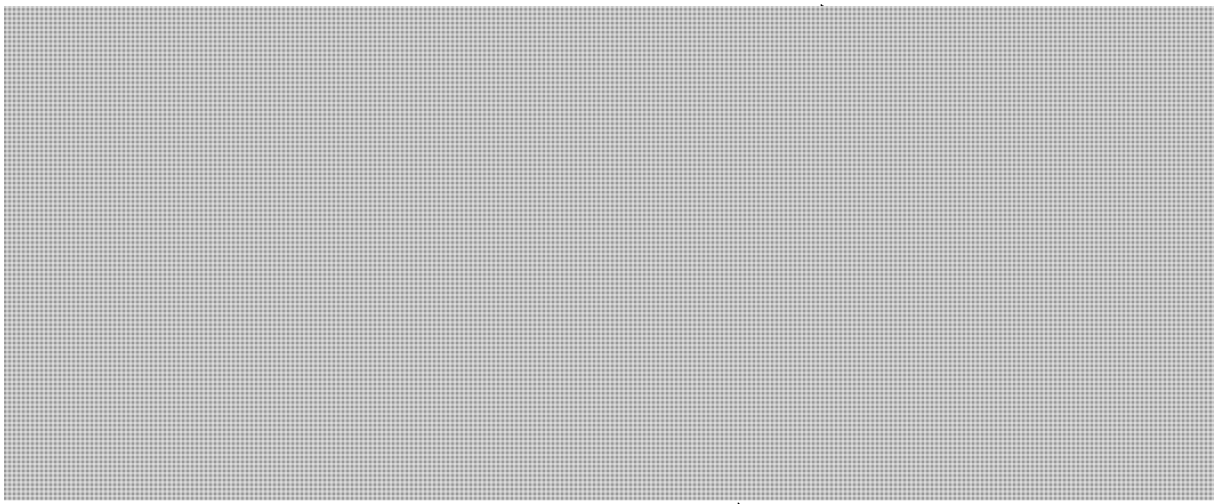
- The cyber-operation cost-benefit equation favours the aggressor. Cyber-operations are cost-effective and deniable, while avoiding direct and open confrontation. They allow the perpetrator to steal from, punish, or coerce their victims and to signal capabilities to other adversaries as a form of deterrence. This makes them an attractive form of asymmetric warfare.

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Transnational Crime

- Traditional national security threats are not the only threat to Canada's national security. Transnational organized crime – those groups that have reached a level of sophistication that allows them to partner with foreign crime organizations – also present a threat. Networks are now international, with partnerships involving other groups around the world.



- Overall, transnational crime threatens the safety and security of Canadians and may also impact the Canadian economy.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.13(1)(a)
s.15(1) - Int'l

Placeholder:

[redacted] to be provided in hard copy to Ministers during the FCM meeting on this topic

Pages 53 to / à 73

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

CYBER THREATS

Strategic Objectives

- Advance the collective understanding of the current cyber threat landscape.
- Reaffirm Canada's commitment to working with allies to respond to global cyber threats and incidents.

Key Messages

Cyber Threats

- Canada has allocated $500 million over the next five years and $109 million per year thereafter to implement its 2018 National Cyber Security Strategy.
- A National Cyber Security Action Plan to implement the fourteen strategy initiatives will be released soon. Some of these initiatives include the development of a Cyber Certification Program for Small and Medium-sized Enterprises, and the creation of the Canadian Centre for Cyber Security and the National Cyber Crime Co-ordination Unit.
- Through collaborative action with partners and enhanced cyber security capabilities, Canada will better protect Canadians from cybercrime, respond to evolving threats, and defend critical government and private sector systems, while fostering innovation and economic growth.

5G

- 5G will enable increased digital interconnectedness, including in our critical infrastructure sectors, thereby introducing new vulnerabilities and attack vectors that will need to be addressed collaboratively.
- Canada is carefully examining the security challenges and potential threats involved in 5G technology, while recognizing the importance that this technology holds in the continued development of a dynamic digital economy.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.13(1)(a)
s.15(1) - Def
s.15(1) - Int'l

- Canada takes the security of Canada's telecommunications networks seriously. In the context of current 3G/4G/LTE networks, a Canadian Security Review Program is in place to mitigate the cyber security risks stemming from designated equipment and services, [redacted]

- The program has led to the exclusion of designated equipment [redacted] in sensitive sectors of Canadian networks.

- Canada will continue to work with allies and private sector partners, including Canadian Telecommunications Service Providers, as 5G technology is adopted by Canadians.

Background

Cyber Threats

The threat and hazard landscape facing Canada has evolved significantly over the last decade. There has been an increase in the number and sophistication of state-sponsored and non-state sponsored cyber activities, including a growing threat of cybercrime against individuals, private and public sector organizations, and government.

At the same time, critical infrastructure sectors are becoming more digitally interconnected and interdependent. Global, distributed, and networked supply chains (including production and delivery processes) are making it increasingly difficult to identify and address vulnerabilities and single-points-of-failure, while the impacts of disruptions are exponentially increased as incidents are no longer isolated to individual organizations and their direct up / downstream partners.

Five Eyes allies continue to collaborate on these issues from both a policy and operational perspective through Five Eyes fora, including the Ottawa 5 (cyber policy), Critical 5 (critical infrastructure) and Usual 5 (cyber operations).

[redacted]

s.13(1)(a)
s.15(1) - Def
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

5G

Canada

Canada's interdepartmental community, led by Public Safety Canada, is conducting an in-depth analysis to provide the Government of Canada with the best possible policy advice on how to secure Canada's 5G wireless telecommunications networks.

The Government of Canada announced in Budget 2019 its intention to propose new legislation and necessary amendments to existing federal legislation in order to introduce a new critical cyber systems framework.

Canadian Security Review Program

While the Government of Canada's review of 5G technology is ongoing, since 2013, the Communications Security Establishment (CSE) has led the Canadian Security Review Program (SRP), which helps mitigate risks stemming from designated equipment and services under consideration for use in Canadian 3G/4G/LTE telecommunications networks, [redacted] CSE defines and monitors the risk mitigation program, accredits third party labs, defines the testing requirements, and reviews proposed architectures to provide tailored advice and guidance to help mitigate risks to Canada's telecommunications networks. To date, this program has led to:

- Excluding designated equipment in sensitive areas of Canadian networks;
- Mandatory assurance testing in independent third-party laboratories for designated equipment before use in less sensitive areas of Canadian networks; and,
- Restricting outsources managed services across government networks and other Canadian critical networks.

The SRP is part of a broader collaborative approach to strengthen cyber security throughout Canada's telecommunications sector, and Canadian TSPs, vendors, and the independent third party assurance providers enter into the equipment review arrangements voluntarily. As part of this voluntary agreement, CSE has worked with a total of 31 telecommunications providers, representing over 99% of the Canadian mobile market to help mitigate the risk of cyber espionage and network disruption through the exploitation of supply chain vulnerabilities in the current 3G/4G/LTE environment.

s.15(1) - Def

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The program has led to the exclusion of designated equipment [redacted] in sensitive sectors of Canadian networks. Annual evaluations of TSPs' architectures have shown year-over-year improvements in adoption of cyber security best practices as a result of this program. The program continues to raise the bar in the telecommunications sector.

Beyond the SRP, CSE also works closely with the Canadian Security Telecommunications Advisory Committee (CSTAC), co-chaired by Innovation, Science and Economic Development Canada and CSE, to allow the private and public sectors to regularly exchange information and collaborate strategically on current and evolving issues that may affect the telecommunications infrastructure.

Allies

Five Eyes allies have either conducted or are conducting similar studies and are making decisions on what equipment can be used in which part of their 5G wireless networks. Australia and New Zealand have both completed their examinations. Australia put in place a legal mechanism to exclude vendors that are subject to extrajudicial direction, while New Zealand has elected to review equipment deployments on a case-by-case basis. The U.K. has yet to complete its examination, and the U.S. continues to put in legal mechanisms related to 5G, while strongly encouraging its allies to carefully weigh the security considerations of 5G technology.

On May 15, 2019, President Trump signed an Executive Order (EO) which outlined a variety of measures on 5G and other Information and Communications Technologies (ICT) intended to protect U.S. national security and economic interests. No country or companies were specifically named. Instead, the EO refers to products "manufactured, supplied, or owned by persons subject to the jurisdiction or direction of a foreign adversary". The EO prohibits U.S. firms from commercial ICT transactions with 'adversaries' who pose a specific threat to U.S. national security, including economic security.

Immediately following the announcement of the EO, the Department of Commerce announced new export control measures targeting Huawei and 68 non-U.S. Huawei affiliates (including Huawei Canada). Consequently, Huawei and affiliates are included on the U.S. export control Entity List. According to the listing, the U.S. government determined "there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States."

With the addition of Huawei and its affiliates to the Entity List, U.S. vendors wishing to sell or transfer technology to Huawei and its affiliates are now required to apply for a licence before doing so. However, the Commerce Department has issued a 90 day temporary general license to prevent the interruption of existing contracts and operational activities.

Drafted: NCSB/NCSD/Lucas Brydges
Consulted: PCO, ISED, CSE, GAC, CSIS, RCMP and DND
Approved by: NCSB/NCSD/Colleen Merchant

Pages 78 to / à 95

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

EMERGING TECHNOLOGIES: INTERNET OF THINGS

Strategic Objectives

- Affirm Canada's commitment, alongside Five Eyes partners, to the protection of our citizens and the security of our economy from cyber threats introduced through emerging technologies, particularly with regard to the Internet of Things (IoT).

- Encourage IoT manufacturers to build cyber security into their products by design to contribute to protection against cyber threats.

Key Messages

- Canada believes that strong cyber security practices incorporated throughout a product's life cycle can help reduce the number of vulnerabilities present in IoT devices.

- Canada is in the process of developing a Cyber Certification Program for Small and Medium-sized Enterprises that is meant to raise the cyber security baseline, increase consumer confidence in the digital economy, and promote international standardization *(Note that this program is broader than just IoT)*.

- Canada recognizes that the lack of cyber security in IoT devices is an urgent global issue requiring action to protect our interconnected and increasingly digital economy.

- Canada readily embraces this important opportunity to bring greater cohesion and alignment with close allies on cyber security and national security.

- Canada looks forward to working closely with industry partners to improve the overall cyber security of IoT devices.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Background

Internet of Things (IoT)

The IoT is comprised of all internet-connected devices. In addition to computers and phones, the IoT has come to include, and add functionality to, many other day-to-day devices and appliances such as refrigerators, watches, lightbulbs, etc. Gartner, a leading research and advisory company, expects that IoT devices will continue to proliferate and will reach over 20 billion devices worldwide by 2020.

Poor security practices make IoT devices attractive targets for cyber criminals and other malicious cyber actors. The exploitation of IoT vulnerabilities can have individual privacy, human rights, economic, and national security repercussions.

Although security concerns largely fall to the personal security and privacy of individuals and families, incidents have also occurred where the exploitation of IoT device vulnerabilities may be used to conduct malicious activity that could impact critical infrastructure. A recent example of this type of activity includes 2016's Mirai Botnet which used IoT device vulnerabilities to conduct a distributed denial of service attack to severely restrict Internet access.

Canada

Canada is working with public and private partners to explore options to enhance IoT security using a combination of education/capacity building, standards, and regulatory efforts. Canada is emphasizing the need for collaboration and holistic, evidence-based policymaking to ensure alignment across industry and with our trading partners. Canada has not issued any specific high-level political statements on IoT.

The recently concluded Canadian Multi-Stakeholder Process on Enhancing IoT Security informs Canada's active international engagement. This year-long effort involved over 12 government departments and agencies and over 200 stakeholders from industry, academia and civil society. The final report outlines the status of the Canadian landscape including stakeholder prioritization of consumer education, standards development and technical solutions related to IoT security. The Canadian IoT initiative led to the creation of a domestic IoT security working group and an international IoT policy platform that connects governments (Five Eyes, EU, Japan, France, Senegal, Uruguay) and industry initiatives (Mozilla, Consumers International, CTA) with active IoT security projects.

Allies

The Ottawa 5 is a Five Eyes cyber security policy forum that meets semi-annually. A Working Group now led by Australia (formerly led by the United Kingdom) was created at the May 2018 forum for the purpose of improving the alignment of approaches to securing IoT devices.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The Working Group drafted the enclosed Statement of Intent to seek agreement at the Ministerial level on a common approach to improving the security of IoT devices, and to signal the intent to work together. The Statement of Intent was endorsed by the Five Eyes at the May 2019 Ottawa 5 forum for approval at the Ministerial level.

Several governments and standards development groups in likeminded countries have introduced measures such as legislation, codes of practice, and formal standards, all working toward strengthened security in IoT devices.

Drafted: NCSB/NCSD/William Meloche
Consulted: ISED, CSE, RCMP
Approved by: NCSB/NCSD/Craig Oldham (CID)

Pages 99 to / à 100

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

CAVEAT: This paper is not to be released until consultation is complete.

Statement of Intent regarding the Security of the Internet of Things

We, the Interior, Homeland Security and Public Safety Ministers of Australia, Canada, New Zealand, the United Kingdom and the United States having met in London, United Kingdom on 29-31 July 2019 to discuss our common security challenges with regards to the Internet of Things (IoT), and how we can best protect our citizens from cyber threats;

Acknowledge that the growth of network-connected devices, systems, and services comprising IoT creates immense opportunities and benefits for our society;

Acknowledge that the number of IoT devices is growing rapidly around the world and that many of these devices lack basic security features;

Acknowledge that vulnerabilities or compromised devices could have serious consequences for individuals, our economies and national security;

Acknowledge that the safety of our citizens and the security of our economies are paramount, and more needs to be done to protect them from risks posed by insecure IoT devices;

Acknowledge that the lack of security in IoT devices is a global issue and that we need to work together to address this problem with common and consistent messaging;

Consider that the potential consequences of security flaws in IoT devices will be magnified in 5G environments; and

Expect manufacturers to develop consumer IoT devices with security built in by design.

Therefore, the undersigned Five Eyes partner nations agree to:

1) Collaborate with respective industry and standards bodies to provide better protection to users by advocating that devices should be secured by design.
2) Actively seek out opportunities to enhance trust and raise awareness of security safeguards associated with IoT devices in our respective nations.
    a. Identify and engage industry partners who share Five Eyes' goals to enhance the security of IoT.
    b. Identify and engage likeminded nations to encourage international alignment on IoT security, unlocking innovation that builds a strong economy that works for everyone.
3) Share information with Five Eyes partners in a timely manner through appropriate channels and arrangements, consistent with international and domestic law, to aid in the overall improvement of IoT security.

29-31 July 2019
London, UNITED KINGDOM

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The Hon Peter Dutton MP
Minister for Home Affairs, Australia

The Hon Ralph Goodale MP
Minister of Public Safety and
Emergency Preparedness, Canada

The Hon Andrew Little MP
Minister for Justice,
New Zealand

The Rt Hon Sajid Javid MP
Her Majesty's Principal Secretary of
State for the Home Department,
United Kingdom

The Hon Kevin K. McAleenan
Acting Secretary of Homeland Security;
United States of America

s.13(1)(a)
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Placeholder:

[redacted] (TBC)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

EMERGING TECHNOLOGIES: DRONES

Strategic Objectives

- Assert Canada's active engagement with domestic and international partners on the efforts to mitigate the threats and risks of Remotely Piloted Aircraft Systems RPAS/drone incidents on the aviation environment.

- Assert Canada's support of the proposed Five Country Ministerial (FCM) deliverables, including the Enhanced Information Sharing Arrangements through the Five Research and Development (5RD) Group and the approach to RPAS/drone manufacturers.

Key Messages

- Canada agrees that given the rapid development of drone and counter-drone/RPAS technology, greater FVEY co-operation amongst our partners and those responsible for addressing this risk would be a benefit to all.

- Counter-RPAS/drone technology alone may not be sufficient addressing the risk at an airport from unlawful interference. As timely actions and coordination can limit the damage and shorten response times for drone mitigation measures, Canada is working closely with airport authorities to develop guidance material that can be used as a national response protocol for airports in the event of an RPAS/drone sighting or incident.

- In terms of manufacturing standards, Canada recommends a cautious approach to regulating manufacturing standards, or technology solutions as counter measures. The regulation of manufacturing processes may introduce unforeseen challenges that could adversely affect operator and manufacturer compliance.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FCM Outcomes Sought for Counter-Unmanned Air Systems (C-UAS) Information Sharing

- Canada agrees that given the rapid development of drone and counter-drone/RPAS technology, greater FVEY co-operation amongst our partners and those responsible for addressing this risk would be a benefit to all.

- Additionally, Canada agrees that further engagement between FVEY and drone manufacturers could be leveraged to assist in the development of mitigations to drone related security risks specific to design and development of drone technology, however ongoing work underway by international standards organizations should also be considered to meet this outcome.

Canada's Collaboration with Domestic and International Partners

- Canada continues to work with domestic and international partners on determining the threats, risks, and countermeasures for potential RPAS/drone implications on the aviation environment. Internationally, this includes Canada working with partners such as the Five Eyes, the US Federal Aviation Administration (FAA), and industry stakeholders, such as the Alliance for System Safety of UAS through Research Excellence (ASSURE), which is part of the FAA's Center of Excellence on UAS, on several RPAS/drone R&D topics.

- For example, Canada is sharing information and potential approaches with the FAA on the development of remote identification policy, standards and requirements to address non-compliant RPAS/drone use, and assist law enforcement and security agencies to make informed decisions on potential RPAS/drone security threats, and a potential means to locate and identify the operator.

- Similar to Europe and the United States, Canada is participating in Joint Authorities for Rulemaking on Unmanned Systems (JARUS) to contribute to the development of standards that support the safe and secure integration of drones into the national airspace system.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Domestically, Canada has established a Government of Canada inter-departmental working group, made up of experts in the field of RPAS/drones, to address the evolving risks of unlawful interference by RPAS/drone to aviation security.

- This working group will focus on identifying what exists in terms of policies, regulatory instruments, and technology for the detection and interdiction of unlawful drones.

- One of the primary strategies of the working group is to collaborate with international partners to gain insight from their experience with drones and what policies and mitigation measures exist to prevent further incidents.

Canada's Approach to Drone Regulations

- Canada has taken an operator-focused approach to regulating drones. Operators of drones weighing between 250g and 25kg, operated in visual line of sight, are required to register their drone and obtain a pilot certificate, which requires an online exam and in some cases, an in-person flight review.

- Canada continues to follow international developments related to remote identification and the potential regulation of drone manufacturers.

- We are in favour of utilizing remote identification as a means of fostering accountability for drone users, and as a future means for enforcement in the event of non-compliance.

- Canada recommends a cautious approach to regulating manufacturing standards, or technology solutions as counter measures. The regulation of manufacturing processes may introduce unforeseen challenges that could adversely affect operator and manufacturer compliance, which may not help States achieve safety or security objectives, and given that the development of the technology used in this environment still requires much research and testing in order to be proven effective.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RPAS Incident Response Protocol

- Counter-RPAS/drone technology alone may not be sufficient addressing the risk at an airport from unlawful interference. As timely actions and coordination can limit the damage and shorten response times for drone mitigation measures, Canada is working closely with airport authorities to develop guidance material that can be used as a national response protocol for airports in the event of an RPAS/drone sighting or incident.

- Canada would welcome the development of a best practices manual or similar guidance to assist airport authorities in countering drone incidents at airports.

- Similarly, a coordinated effort by the FCM to share information on best practices, lessons learned and new techniques that can be leveraged during the development of incident response protocols would also be welcomed by Canada.

- For example, in Canada, the RCMP Counter Unmanned Aerial System (CUAS) program conducts numerous CUAS operations, specifically for the protection of Internationally Protected Persons (IPPs). Gaps, lessons learned and best practices could be shared with partners from the FVEY in order to educate and improve CUAS operations and capabilities.

Canada's Views on the Ministerial Deliverables

- With respect to the ministerial deliverable on information sharing, Canada would be supportive of the Enhanced Information Sharing Arrangements deliverable proposed in the concept note.

- Furthermore, Canada is supportive of leveraging international information-sharing fora to exchange scientific and technological developments to inform holistic threat analysis.

- Canada is also supportive of the proposed FCM approach to RPAS/drone manufacturers, as industry in Canada have indicated that they are supportive of receiving government guidance on this topic.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Background

The topic of Emerging Technologies will include a discussion on the subject of **Counter-Unmanned Air Systems** or also known as Remotely Piloted Aircraft Systems (RPAS). RPAS or "drones" consist of an unmanned aircraft and its associated elements, including a remote pilot (typically ground-based) and the system of communication between the two. In Canada and around the world the drone industry is growing at a rapid pace. Over the past decade, technology advancement has made drones more capable and acquisition and use more affordable and accessible for the general public.

This increased accessibility has led to renewed attempts by malicious actors, including organized crime and terrorist groups, to exploit drones for nefarious purposes. This topic has been a growing concern as there have been an increasing number of drone incidences at international airports, specifically the Gatwick incident, which lasted over 30 hours and disrupted the travel of over 140,000 passengers, and is estimated to have cost the airlines 87.49 million CAD.

Canada's approach to addressing nefarious RPAS/drone incidents around airports is a shared responsibility. At the federal level, various departments are responsible for particular aspects of a RPAS/drone incident at an airport. For example, Transport Canada is responsible for airport security related incidents and the threat to aviation security, such as the Gatwick event, while Public Safety Canada is the lead for countering and responding to threats to critical infrastructure, public gatherings and other similar public safety and security concerns. Canada recognizes the importance of working together, to share information, and a common vision to adequately address this challenge.

From a C-UAS perspective, Transport Canada is not currently in a position to certify equipment or regulate airports or entities (e.g. NavCanada) to conduct counter-measure activities. Canada has conducted some research activities and we continue to carry out additional testing on counter-measure technologies, however research is still preliminary, and we are therefore proceeding with a degree of caution.

Drafted: Transport Canada/Program Development/Aviation Security/Justin Jedlinski
Consulted: Transport Canada/Civil Aviation and RCMP
Approved by: Transport Canada/Safety and Security/Kevin Brosseau

Pages 109 to / à 110

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

BORDERS AND IMMIGRATION: ASYLUM SYSTEMS ABUSE AND FRAUD

Strategic Objectives

- Support the Minister of Immigration, Refugees & Citizenship Canada (IRCC), as the lead on the topic of Asylum Abuse and Fraud.
- Agree to the sharing of best practices in addressing unfounded claims at ports of entry.

Responsive Key Messages Only (No proposed intervention as this is an IRCC lead)

Canada's Approach to Borders and Asylum Systems Abuse And Fraud

- Canada's public safety portfolio, including the Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency (CBSA) works hand-in-hand with our immigration colleagues to detect, discourage and manage continued volumes of irregular migration abroad, ensure preparedness for influxes at the border and maintain public confidence in Canada's border management and immigration program.
- The Government of Canada is enhancing its border management to deter irregular migration, and investing in the asylum system to ensure decisions are fast, fair and final.
- If asylum claimants who have crossed regularly or irregularly are found not to need Canada's protection, the Canada Border Services Agency will ensure their removal.

Background

Canada's asylum system provides lifesaving protection to those with well-founded fears of persecution. However, there are a range of factors contributing to the abuse of our asylum system. This includes consultants and agents who facilitate fraudulent travel and organised criminal syndicates who work to facilitate irregular people movements and conduct illegal activities like human smuggling and trafficking.

Canada has seen a significant rise in asylum claim intake (regular and irregular) with approximately 50,000 claims in 2017 and a historic high of over 55,000 claims in 2018.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

In an effort to improve the efficiency of Canada's asylum system, Budget 2019 announced $1.18 billion over 5 years, starting in 2019-2020, and $55.0 million per year ongoing to enhance the integrity of Canada's borders and asylum system. These investments will support the Government's Border Enforcement Strategy, and will increase the asylum system's capacity to provide timely protection to refugees and ensure failed asylum claimants are removed, faster. The Government's approach has three main pillars:

1) Manage arrivals at the border, while ensuring the safety of Canadians, and maintaining contingency plans in the event of an influx of asylum seekers;
2) Detect and discourage misuse of Canada's visa system, by preventing travel to Canada by individuals who may not be legitimate temporary visa applicants; and
3) Invest in the asylum system for a fast, fair and final system by processing more asylum claims faster and by removing those who do not need Canada's protection

A specific measure that has a Five Country impact is a legislative change to render those who have made asylum claims in countries with which Canada has an immigration information sharing agreement in place – namely the Five Countries – as ineligible to make an asylum claim in Canada.

The Five Country Ministerial (FCM) discussion will explore opportunities for more enhanced strategies and to better develop multilateral engagement between the Five Eyes partners to preserve the integrity of protection regimes.

Drafted: SPB/IPPD/Daniel Lay
Consulted: IECERPD
Approved by: CBSA/SPB/Kathleen Thompson

Pages 113 to / à 119

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

BORDERS & IMMIGRATION: DATA SHARING

Strategic Objectives

- Indicate support for the continued work on the Border of the Future Strategic Plan which will be implemented under the leadership of the Border 5 and Migration 5, and commit to maintaining momentum and investment over the long-term.
- Note the importance of data sharing and protecting privacy as the foundational basis for the Border of the Future.
- Exchange views on how Five Eyes data sharing impacts domestic public trust.

Key Messages

- *Additional key messages and background material relating to "Criminal Information Sharing and Travelling Sex Offenders" has been provided separately should the discussion move onto that topic.*

Data Sharing

- Alignment across the Five on data sharing and privacy is essential for building the Border of the Future.
- Data sharing is a key enabler for travel and trade facilitation, border management, and protection of our citizens. Data sharing between the Five Eyes is an important prerequisite to both enhance security and foster economic prosperity. Developing common and standard approaches to data sharing can increase efficiency and cost-savings, particularly as there are increasing volumes of international flows of goods and people.
- As a foundational piece to advance the Border of the Future, it will be important to examine where we can enhance data sharing across the Five Eyes. Canada is exploring opportunities to develop a common approach to data across various streams such as commercial, traveller, postal, and immigration across the five.
- Canada is open to developing systems to share the relevant data, such as biometrics, with its partners. In the border context, the Canada Border Services Agency believes that facial biometrics is the path forward, as it is aligned with existing standards and practices and it allows for a low touch

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

processing model. This data sharing would require significant public engagement and stakeholder consultation.

- I endorse the development of a forward work plan for Border of the Future under the direction of the Migration 5 and Border 5 Heads in order to ensure that we continue to advance the work on this important forward-thinking initiative and that we embrace the use of new and emerging technologies to assist us in addressing the sharing of data.

Data and Privacy

- Common principles for privacy and data security pave the way for a practical framework to expand data sharing towards the 'known to one, known to all' vision.

- A clear and easy to understand set of common principles related to privacy that guide the protection of personal information and data will strengthen our security regimes, as well as ensure public awareness and build confidence in government data management.

- Canada has robust privacy legislation, though we recognize there is a need to address public concerns in new emerging areas such as data analytics and artificial intelligence

The Social Contract

- Expanded data and information sharing requires strong public trust. When citizens release their personally identifiable information to government agencies there is an implicit 'social contract' that the government will ensure adequate privacy safeguards and data sharing protocols will be respected.

- Although governments maintain very robust privacy regimes and safeguards, some citizens remain hesitant to trust their personal information to public institutions.

- To ensure a successful transition to the Border of the Future, Governments will need to communicate to their citizens the importance of sharing certain data, with whom that data is shared, and how it is used. Therefore, transparency around data sharing will be fundamental to building public

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

trust. This transparency is aligned with the Government of Canada's objectives, as open data is already a priority of the Government.

Background

Border of the Future and Its Benefits

The Border of the Future is an ambitious and collaborative program of work that aims to create a touchless border built on key pillars, including a 'known to one, known to all' approach. Achieving this touchless border will require, among other things, real time data sharing and a common approach to privacy protections amongst the Five Eyes countries.

Overall, the program of work will benefit the Five Eyes countries economically through facilitation of legitimate trade and travellers, while also improving national and global security outcomes through better targeting and interception of those posing harm.

Border of the Future 2030

The *Border of the Future Strategic Vision 2030* (the Strategic Vision) was endorsed at the 2018 Five Country Ministerial. The Strategic Vision proposed outcomes to improve our ability to protect our borders integrity through:

- **Ensuring that travellers and goods are processed well before they reach a physical border** and enabling us to detect and manage risks ahead, at and after, the border;
- **Facilitating the movement of legitimate goods and travellers between our countries** and improved targeting of high risk entities;
- **Enhancing our enforcement and risk capabilities** to meet the challenges of sophisticated threats, global and complex supply chains, and higher volumes; and
- **Drawing on our collective capabilities, and harnessing rapidly-evolving technology** to better manage border and national security challenges.

At the 2018 Five Country Ministerial, Ministers subsequently tasked the development of the *Border of the Future Strategic Plan 2019-30* (the Strategic Plan), which documents a number of initiatives that are required to achieve the Strategic Vision's outcomes of a touchless border by 2030. In developing the Strategic Plan, it has become evident that privacy and the ability to share data is fundamental to the success of the Border of the Future. Addressing these foundational initiatives will enable the remaining initiatives to be more easily and effectively implemented.

The CBSA is in a process of institutional renewal for the purpose of helping travellers and traders follow the regulations; speeding up border crossings for low-risk travellers and goods; and targeting and stopping the greatest threats using analytics. These goals are aligned with the Strategic Plan and vision of using technology to create a touchless border.

The development and implementation of the Border of the Future program of work from 2019 to 2030 requires strong governance arrangements.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Drafted: CBSA/SPB/IPPD/Peter Bito
Consulted: CBSA/IRCC
Approved by: CBSA/SPB/Kathleen Thompson

Pages 124 to / à 130

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 131 to / à 133

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l, 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 134 to / à 148

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

DINNER DISCUSSION: SOCIAL INTEGRATION, INCLUSION, and IDENTITY

Strategic Objectives

- Reassert Canada's interest in discussing social cohesion and inclusion, while ensuring a focus on relevant aspects of these concepts.

- Support the sharing of best practices in fostering inclusion and social cohesion, as well as identifying and addressing signs of social fracturing.

Key Messages

Canada's Approach to Integration, Inclusion and Diversity

Defining Social Cohesion

- Canada takes a broad approach to social cohesion and inclusion, one that encompasses society as a whole.

- Factors such as economic shifts, the effects of traditional and social media, demographics/social change, and decline in trust, among others, all have a bearing on social cohesion.

- Some current areas of concern for Canada include the recent rise in police-reported hate crime, as well as polling results indicating that a significant percentage of Canadians view our society as divided.

- And while indicators suggest that Canadians trust key institutions more than in many similar countries, there are important segments of the population where experiences of sectors such as health and justice are characterized by discrimination.

How Canada is working to improve Social Cohesion and Inclusion

- As my colleague Minister Hussen has noted, there are a number of initiatives in Canada which bring together inclusion and social cohesion objectives, for example, through efforts to reduce poverty, engage citizens in digital literacy, combat racism, and advance reconciliation between Indigenous and non-Indigenous peoples.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- In the national security sphere, our security and intelligence community has renewed its commitment to a more bias-sensitive, inclusive approach to analysis and decision-making in security-related work, reflecting the importance Canada places on gender, diversity and inclusion.

- Canada is also taking measures to prevent and address threats to social cohesion such as violent extremism, terrorism, hate speech, hate crime, and foreign interference.

- For example, as part of Canada's new Anti-Racism Strategy, which is led by the Department of Canadian Heritage, Public Safety Canada will be working to help address hate crimes and hate speech. Priority areas include better understanding the connections between online and offline behaviour of those committing hateful acts, as well as the resulting harms of such activity, and applying this greater evidence base to support more effective prevention and intervention.

- Where Canada is currently facing challenges, it is working to identify measures to detect signs of social fracturing, as well as effective policy and program tools to foster inclusion and strengthen social cohesion.

Potential Areas for Collaboration

- [redacted]
- [redacted]

- Canada supports the sharing of information on individual and community-level vulnerabilities relevant to specific security concerns linked to issues of exclusion, polarization and fracturing.

- There is a need to determine how safety and security organizations can ensure their roles and approaches contribute to social cohesion.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Background

Canadian Context:

The concept of social cohesion aims to capture the qualities of a well-functioning society characterized by strong levels of trust and sense of belonging, widespread well-being and opportunities to succeed, and limited presence and impact of exclusion and marginalization. Inclusion and integration, therefor, can be viewed as means of reaching social cohesion.

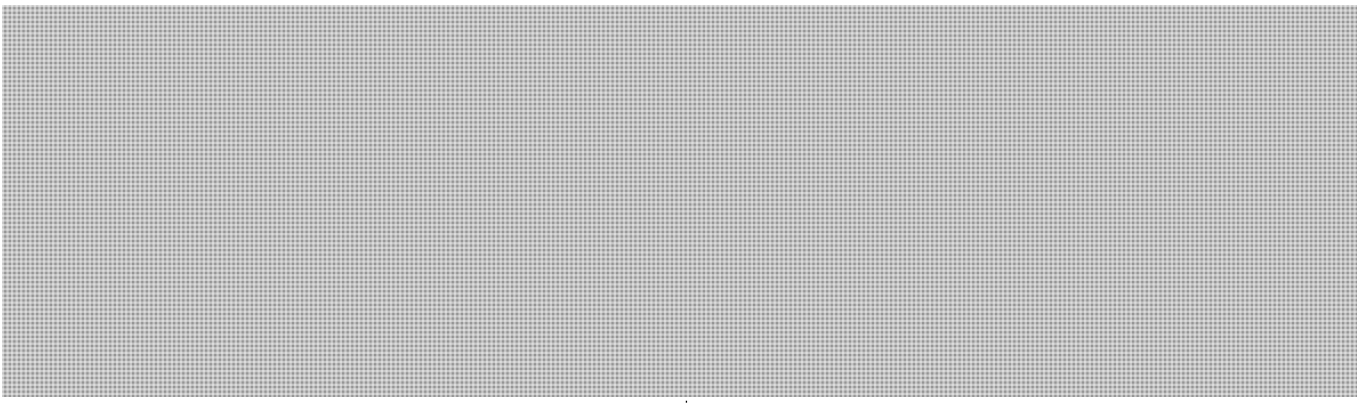
Social cohesion and inclusion are topics that are of important interest for Canada, including through recent concerns about social fracturing. For example, the social polarization that is being witnessed in like-minded countries has coincided with a rise in hate crime domestically. In Canada, hate crime was at an all-time high in 2017 (according to Statistics Canada). Polling in 2018 found that almost two-thirds of Canadians believed that Canada was divided (Ipsos). And while an annual survey of trust and credibility in 27 countries found Canadians in 2019 to trust their key institutions more than citizens in like-minded countries such as the United States, the United Kingdom, France, and Australia, the same survey found that only 56 percent of the general population in Canada trusts its institutions will 'do the right thing,' resulting in Canada being classified as 'neutral' on trust, rather than a clear 'trust' state (Edelman Trust Barometer).

Currently, Canada has a number of initiatives in place which foster inclusion and cohesion. These include: reconciliation efforts, the Poverty Reduction Strategy, the National Housing Strategy, the Multiculturalism Strategy, and the new Anti-Racism strategy. In addition, Public Safety's work on enhancing the application of GBA+ within the S&I community brings greater awareness to security practitioners regarding the need for social cohesion. Work in this area is not new, however, recent initiatives are aiming to more rigorously and systematically apply GBA+ as an approach to security-related work. An example is the recently released National Strategy on Countering Radicalization to Violence, which considers gender dynamics as an important dimension for better understanding, preventing, and countering violent extremism.

This said, additional work is needed in order to accurately identify signs of social fracturing, particularly those that pose significant security concerns, as well as policy and program tools which could be utilized to foster inclusion and strengthen social cohesion.

Currently, commonly used measures of fracturing involve opinion polls, socio-economic trend data, and hate crime data. Such measures tend to be too broad and too limited, however, to inform policy and program efforts to identify and preserve what already protects against fracturing, as well as to proactively intervene to promote social cohesion.

International Context:



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Drafted: PACB/CCCEPV/Catherine Giguere
Consulted: NCSB/CSCCB/PCH/RCMP and IRCC
Approved by: PACB/Wherrett

Pages 153 to / à 155

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

INDUSTRY ROUNTABLE ON CHILD SEXUAL EXPLOITATION AND ABUSE

Strategic Objectives

- Reassert Canada's support to make digital industry more accountable in the fight against child sexual exploitation and abuse online.

- Engage in frank discussion with the digital industry to encourage them to develop solutions to the proliferation of child sexual exploitation and abuse on their platforms.

Key Messages

Engagement with Digital Industry to Combat Online Child Sexual Exploitation and Abuse Online

- Canada welcomes digital industry engagement with the Five Eyes and looks forward to working together to find solutions to address child sexual exploitation and abuse online.

- Canada encourages further dialogue with the digital industry on the issue of global industry responsiveness toward the prevention and removal of child sexual exploitation images.

- Canada agrees that the digital industry, as a whole, should be guided by a set of voluntary principles that provide a clear and consistent framework in the fight against online child sexual exploitation and abuse.

- Canada encourages digital industry to continue to engage with the Five Eyes through the digital industry Engagement Senior Officials Group.

- Canada believes the digital industry has an obligation to continue to develop tools to combat all forms of online child sexual abuse and exploitation, including livestreaming of child sexual abuse and luring and grooming, and to build on recent developments,

- Canada encourages digital industry to share good practices on prevention and education with smaller companies.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Canada is committed to working closely with digital industry, including through DIESOG, to combat this heinous crime.

Background

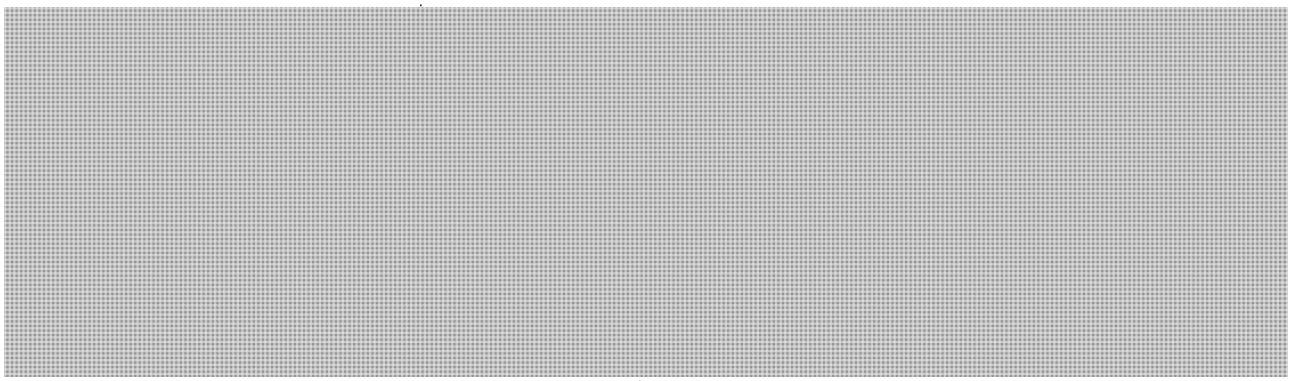
Industry Participants

- Facebook – Antigone Davis, Director Global Head of Safety
- Google – Leslie Miller, Vice President Global Policy
- Microsoft –Jacqueline Beauchere, Chief Online Safety Officer
- Snap - Jennifer Park-Stout, Vice President Global Policy
- Twitter – Katy Minshall, Head of UK Government, Public Policy and Philanthropy
- Roblox – Remy Malan, Vice President of Trust and Safety and Chief Privacy Officer

Digital Industry Engagement

Online child sexual exploitation (CSE) is one of the most pressing public safety issues facing society today. Addressing this crime is a priority for Canada and for key allies, as reflected in the discussions at the 2018 FCM meeting in Australia. Digital industry representatives were invited to participate in a joint meeting with FCM ministers, however, none were able to attend. FCM ministers issued a joint statement which included a commitment to work with digital industry to prevent online CSE, including live-streaming of child sexual abuse.

The digital industry Engagement Senior Official Group (DIESOG) was created to monitor and track digital industry progress related to the FCM statement on Countering the Illicit Use of Online Spaces. This includes close collaboration with digital industry to assess legal, policy and operational issues around the pro-active takedown by industry of Child Sexual Abuse Material (CSAM), and to further develop tools, technologies and techniques that could be used for this purpose and to reduce CSAM from being traded, distributed and shared. The Canada Centre for Community Engagement and Prevention of Violence at Public Safety Canada is the Canadian representative on DIESOG. The Serious and Organized Crime Division within Public Safety (PS), which leads the National Strategy for the Protection of Children from Sexual Exploitation on the Internet (National Strategy), sits on the Informal Working Group on Digital Engagement which supports Canada's participation in the DIESOG.



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

National Strategy for the Protection of Children from Sexual Exploitation on the Internet

The National Strategy for the Protection of Children from Sexual Exploitation on the Internet was launched in 2004. Public Safety Canada is the lead for the National Strategy and partners with the Royal Canadian Mounted Police, Justice Canada and the Canadian Centre for Child Protection (C3P), a not-for-profit organization responsible for operating Cybertip.ca, the national tip-line on the National Strategy. PS coordinates and oversees the implementation of the National Strategy, develops online CSE policy, and provides contribution funding to C3P for the operation of Cybertip.ca, as well as to other non-governmental organizations for targeted public awareness activities.

The National Strategy was renewed on an ongoing basis in 2009. That said, the technological landscape has changed considerably in recent years and technological advances have facilitated the easy, borderless access to, and sharing of, large quantities of images and videos of children being sexually exploited. In addition to the growing volume of child sexual abuse material online, technological advances have led to emerging new trends such as self-generated materials and sexting, sextortion, grooming and luring, live child sexual abuse streaming, and made-to-order content. The proliferation of online child sexual exploitation material demonstrates the need for the Government to continue to strengthen its response to this complex, escalating issue.

To this end, through It's Time: Canada's Strategy to Prevent and Address Gender-Based Violence (the GBV Strategy), Public Safety Canada received additional funding of $1.3 million annually, on an ongoing basis, in Budget 2017 to:

- Develop further public awareness;
- Enhance policy coordination and research; and,
- Enhance Cybertip.ca's capacity to support, through Project Arachnid, an increased rate of removal of child sexual abuse material online.

Budget 2018 announced further investment for the GBV Strategy of $5.8 million annually, on an ongoing basis, to enhance the RCMP's National Child Exploitation Coordination Centre's investigation capacity.

Building on investments in Budgets 2017 and 2018, Budget 2019 announced a further investment of $22.24 million over three years, starting in 2019–20, to combat child sexual exploitation on the Internet. This funding will support Public Safety Canada's efforts to raise awareness of this serious issue, reduce the stigma associated with reporting, increase Canada's ability to pursue and prosecute offenders, and work together with industry to find new ways to combat this crime.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Initiatives funded through Budget 2019 will be rolled-out starting in the 2019-20 fiscal year, and will support a number of other Government priorities, including Canada's Strategy to Prevent and Address Gender-Based Violence.

PS' digital industry engagement efforts will support and reinforce Canada's international commitments to work with digital industry to find solutions to child sexual exploitation and abuse online.

Drafted: CSCCB/LEBS/Mathilde Briere-Audet
Consulted: JUS, RCMP
Approved by: CSCCB/Burack

Pages 160 to / à 167

are withheld pursuant to sections

sont retenues en vertu des articles

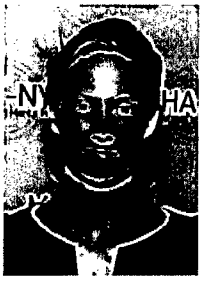
13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BIOGRAPHIES – Digital Industry Roundtable Participants



Antigone Davis

Facebook – Director, Global Head of Safety

Antigone Davis is Head of Global Safety at Facebook, where she works with internal teams at Facebook and with external safety organizations and government bodies to ensure that Facebook remains a leader in online safety and that stakeholders understand the steps Facebook takes to promote safety online.

Antigone also spearheads the efforts of Facebook's Safety Advisory Board, a team of leading safety organizations from around the world who provide Facebook with cutting edge research and advice on best practices, as well as its Global Safety Network.

She serves on the International Advisory Board for WePROTECT as well as the boards of the National Cybersecurity Alliance, the Family Online Safety Institute, and the National Network to End Domestic Violence.

Prior to joining Facebook, Antigone spent 10 years working for a State Attorney General. As Senior Advisor to the Attorney General, she helped establish the office's first online privacy and safety unit, and led the National Association of Attorney General's 2012-2013 presidential initiative "Privacy in the Digital Age." Before serving in the public sector, Antigone used her juris doctorate from the University of Chicago Law School as a corporate attorney in Chicago.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Leslie Miller
Google – Vice President Global Policy

Leslie Miller serves as acting head of global public policy for Google, overseeing strategy and operations for a team of 200+ employees worldwide. During her eight-year tenure at the Internet Company's headquarters, Miller has led teams tasked with setting global public policy strategy as well as public advocacy efforts. Her focus is building and executing campaigns around tech policy and regulatory outcomes that support the industry (eg. autonomous vehicle policy). Miller previously led Google's corporate communications team and is a seasoned spokesperson that specializes in crisis response.

Prior to joining Google, Miller spent time in the trenches of Democratic politics focused on grassroots organizing and political communications. She served on Barack Obama's successful 2008 presidential campaign and began her career at NBC News.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Jacqueline Beauchere
Microsoft –Chief Online Safety Officer

Jacqueline Beauchere is the Chief Online Safety Officer at Microsoft Corporation. In this role, Ms. Beauchere is responsible for all aspects of Microsoft's online safety strategy, including cross-company policy creation and implementation, influence over consumer safety features and functionality, and communications to and engagement with a variety of external audiences.

She currently serves as an international advisory board member to the U.K. government-sponsored WePROTECT Global Alliance to End Child Sexual Exploitation Online; is a member of INHOPE's Advisory Board, as well as the Better Internet for Kids Advisory Board led by the European Commission. She has previously served as Microsoft's representative to the boards of directors of the National Cyber Security Alliance, the Technology Coalition, and the Family Online Safety Institute.

Ms. Beauchere has spent nearly 20 years at Microsoft leading various groups and efforts that evangelize the company's commitment to safer, more trusted online experiences for people of all ages and technical abilities.

Before joining Microsoft, Ms. Beauchere was an attorney in private practice in New Jersey, New York, and Washington, D.C. A second-career lawyer, she spent 12 years as a real-time financial news correspondent and editor-in-charge, most recently with Reuters America, Inc., in New York.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Jennifer Park-Stout
Snap - Vice President Global Policy

In January 2017, Jennifer left the US Department of State for the private sector to become Snap's new Head of Global Public Policy. Now she's in charge of deepening Snap's ties with Washington DC and other governments where the company operates.

She served as Deputy Chief of Staff to Secretary of State John Kerry. She also served in a number of capacities both in and out of government. Most recently, Jennifer was Chief of Staff to Under Secretary of State for Public Diplomacy and Public Affairs Richard Stengel. Prior to that, she was Special Assistant to the President in the White House Office of Legislative Affairs.

From 2012 to 2013 as Vice President of International Government Relations for MetLife, Jennifer supported government and industry relations and international business segments in the Asia Pacific. From 2010 to 2012, she was a Deputy Assistant Secretary in the East Asian and Pacific Affairs Bureau at the State Department, leading the bureau's public affairs and public diplomacy strategy.

Previously Jennifer was Senior Advisor and Director of Senate Affairs in the Bureau of Legislative Affairs at the State Department and spent 11 years on Capitol Hill, working as a legislative aide to then-Senator Joseph Biden on the Senate Foreign Relations Committee, Senator Patrick Leahy on the Senate Committee on Appropriations, Subcommittee on State and Foreign Operations, Senator Jim Webb, and Representative James Moran.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Katy Minshall

Twitter – Head of UK Government, Public Policy and Philanthropy

As head of the Government, Public Policy and Philanthropy team at Twitter, Ms. Minshall guides the team to focus on public policy issues posed by the continuing spread of digital technology and web-based communications services around the world. These issues range from freedom of expression, online safety, intellectual property, copyright, privacy and Internet freedom.

The Public Policy team's efforts involve working directly with NGOs active in the areas of digital inclusion, freedom of expression, online safety and security, equality, women and minorities in tech, and emergency services/disaster mitigation and recovery. Ms. Minshall and her team also work to showcase the role of Twitter in government and for civic participation. As the head of the UK branch, her team specifically monitors public policy issues of importance to Twitter and its users in the UK, including national legislative and executive branches, UK government bodies and public institutions.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Remy Malan
Roblox –Vice President of Trust and Safety and Chief Privacy Officer

Remy Malan serves as both Vice President of Care & Safety and Chief Privacy Officer at Roblox. In his role as VP of Care & Safety, Remy is focused on identifying and implementing best practices to ensure that Roblox is a safe and civil environment for our thriving community of players and creators across the world. He leads our customer care, content moderation, and online safety initiatives, developing industry-leading technology to promote positive online behavior among kids and teens. Remy also leads the company's Privacy Office and its mission of protecting the privacy of the Roblox community.

Remy brings over 25 years of industry experience to the executive team, having built a reputation for establishing high-performing, customer-focused organizations at a number of technology companies. Prior to joining Roblox, Remy was the Chief Customer Officer at SugarCRM where he was instrumental in ensuring the success of its customers' CRM implementations. He also held other customer-facing executive roles at companies such as Teleplace, a 3D collaboration environment featuring user-generated content for education and training, and AOL Time Warner. Remy is passionate about creating great experiences for customers and finding new ways to engage with them.

s.13(1)(a)
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

BRIEFING NOTE FOR THE MINISTER

COUNTERING FOREIGN INTERFERENCE

Strategic Objectives

- Reaffirm Canada's support for the commitment agreed to at the last FCM to share developments in our respective approaches to confronting the foreign interference challenge. [redacted]
- Reiterate the inclusion of Australia and New Zealand into the information sharing aspect of the G7 RRM, and encourage the FCM members to identify opportunities to leverage existing mechanisms to further reinforce this commitment of information sharing.
- Share Canada's approach to securing elections and addressing the broader threats of hostile state activity.
- Support Five Eyes' efforts to expand collaboration on countering foreign interference broadly defined to include threats to our economy, academia, communities, and other levels of government, among others.

Key Messages

- *You will co-lead this session with Minister Dutton from Australia. It is expected that Minister Dutton will speak first. Your suggested opening remarks are attached separately.*

Background

[redacted]

Ahead of the 2019 elections, Canada passed amendments to its federal election law to prohibit activities by foreign states such as: intimidation of voters; spending money directly on partisan activities, political advertising or polling; or using third parties to conceal their support for

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

those activities. The amended law will also require online platforms such as social media sites to publish a registry of all partisan or other political advertising they carried and who authorized the ads, and to keep that information available for a minimum of two years after the ads are posted. Google has publicly stated that rather than develop this registry, it will be banning all political advertising on its platform. Facebook has announced that it will comply.

On 30 January 2019, Minister Gould, alongside Minister Sajjan and yourself, outlined Canada's plan to safeguard the October 2019 federal election. The plan included the following measures across four pillars:

Enhancing citizen preparedness

- Establishing the Critical Election Incident Public Protocol, a mechanism for communicating with Canadians during the writ period in a clear, transparent, and impartial manner about incidents that threaten the integrity of the election.
- Creating the Digital Citizen Initiative to support digital, news and civic literacy programming and tools;
- Increasing the reach and focus of Get Cyber Safe, the national public awareness campaign created to educate Canadians about cyber security and the simple steps they can take to protect themselves online, to include greater linkages to cyber threats to Canada's democratic processes; and
- Releasing an update to the Cyber Threats to Canada's Democratic Process, the public assessment of threats to Canada's elections, political parties and politicians, and voters.

Improving Organizational Readiness

- Offering additional cyber security technical advice and guidance to political parties to enhance security.
- Offering classified threat briefings to key leadership in political parties to promote situational awareness and help them to strengthen internal security practices and behaviours.

Combatting Foreign Interference

- Continuing efforts through the G7 Rapid Response Mechanism to strengthen coordination across the G7 in identifying, preventing and responding to threats to G7 democracies.
- Launching a Security and Intelligence Threats to Elections (SITE) Task Force to improve situational awareness related to Canada's electoral processes and help Government assess and respond to threats.
    - Task force is comprised of the CSE, CSIS, RCMP and Global Affairs Canada and is now activated and operational.
- Creating a Critical Election Incident Public Protocol to establish a transparent, non-partisan process to inform Canadians of significant threats to the integrity of the 2019 Election.
    - **Scope**: limited to incidents that fall within the writ period.
    - **Threshold**: exceptional circumstances that impair a free and fair election, based on a single incident or a culmination of incidents. Considerations include:
        - the degree of confidence in the intelligence or information;

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- the degree to which incident(s) undermines democratic rights;
- the potential of the incident(s) to undermine election credibility; and
- the potential impact of the incident(s) on the national interest.

- **Who**: group that makes the determination is comprised of five principals: Clerk of the Privy Council; National Security and Intelligence Advisor; Deputy Minister of Public Safety, Deputy Minister of Justice and Deputy Attorney General; and the Deputy Minister of Global Affairs Canada.

Expecting Social Media Platforms to Act

- Engaging with social and digital platforms to encourage them to implement specific measures to increase transparency, authenticity, and integrity on their platforms, and combat the spread of disinformation.
- Introducing the Canada Declaration on Electoral Integrity Online, which a number of the major platforms have pledged to fulfill to establish a common understanding of the responsibilities of both platforms and Government about their respective responsibilities in the online democratic space.

[redacted]

Drafted: NCSB/NSOD/[redacted]
Consulted: RCMP/CSIS/PCO
Approved by: NCSB/Beauregard

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Five Country Ministerial 2019

Session 6: Countering Foreign Interference

Remarks

for

The Honourable Ralph Goodale

Minister of Public Safety and Emergency Preparedness

Tuesday, July 30, 2019

London, United Kingdom

Word count for remarks: 842 (7 minutes @ 120wpm)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Election Security and Protecting Democracy

- Canada remains supportive of the Five Eyes sharing developments in our respective approaches to confronting the foreign interference challenge. We believe that it is important to work together to counter this threat by sharing best practices, and collaborating where appropriate.

- Canada supports the work undertaken over the last year to implement this commitment, including the Countering Foreign Interference Summit hosted by Australia, which allowed partners from around the world to share their experiences and their solutions to address this threat.

- We believe that the Five Eyes, and like-minded countries, can present a unified response to acts of foreign interference, when appropriate. The unanimous condemnation by Five Eyes partners, as

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

	well as other around the world, in response to the poisoning incident in Salisbury by Russia is an example of that. Similarly, the public statements issued by our respective countries condemning China's global hacking campaign targeting companies and government agencies to steal intellectual property and sensitive commercial data were made more powerful by their coordination. • Canada faces threats to its democratic institutions from cyber (e.g. hack and leak), online (e.g. disinformation campaigns through social media), and from more traditional human-based sources. As such, the Government of Canada has made protecting the integrity of our federal election in October 2019 a top priority. • Canada passed amendments to its federal election law in December 2018 to prohibit partisan activities by foreign states such as: spending money directly on partisan activities, political advertising or polling; and to prohibit third parties from using foreign funding for partisan activities and advertising. • To counter disinformation and improve

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

transparency, the amended law requires major online platforms such as social media sites to publish a registry of all partisan and election advertising they carried and who authorized the ads. That information must be publicly available for a minimum of two years after the ads are posted.

- More recently, my colleague, the Minister of Democratic Institutions, in collaboration with the Minister of National Defence and myself announced other new measures to improve our readiness to counter election interference.

- Agencies within my portfolio play a key role in this regard. For example, the Canadian Security Intelligence Service (CSIS), has longstanding investigations into foreign interference threat activities targeting democratic processes and institutions across Canada. Its provision of intelligence and assessments to senior levels of government, as well as to Canada's arms' length election agency, allows for informed decision making when responding to and developing policies to address these threats.

- Beyond this broader role, some specific measures

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

include:

- Participating in the Security and Intelligence Threats to Elections (SITE) Taskforce, established to improve situational awareness and help the Government assess and respond to threats. In addition to CSIS and the RCMP, this task force includes the Communications Security Establishment and Global Affairs Canada; and

- Advising political parties on how they may be affected by foreign interference and informing those parties on how to protect themselves.

- Other measures include establishing the Critical Election Incident Public Protocol as a mechanism to inform Canadians through a clear, transparent, non-partisan manner if there is a threat to the integrity of the 2019 election. If the threat meets a high threshold, five senior public servants would request that relevant intelligence agency heads make a public announcement to provide appropriate information to Canadians.

- We have also taken action to enhance the preparedness Canadians in general. For example,

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

we have established the Digital Citizen Initiative to support digital, news and civic literacy programming and tools.

- The Government is also increasing its public messaging about risks to the election to increase awareness of the challenge. I and other Ministers and senior security officials have been putting the spotlight on foreign interference in a number of public speeches since the fall of 2018.

- Canada looks forward to sharing our experience following the October 21, 2019 General Election.

Facing Threats from Hostile State Activity

- Beyond addressing threats to the integrity of our electoral process, Canada is examining a range of options to more broadly address the longer term threat posed by foreign interference and espionage, in areas such as the economy, academia, and other levels of government, among others.

- Foreign actors often approach their interference activities from a broad integrated perspective, viewing political interference, economic espionage and cyber-enabled operations as part of a whole.

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

[redacted] I look forward to continuing this work, both as a Five Eyes group, and with other like-minded countries.

Word Count: 842 words

Time: 7 minutes

Pages 184 to / à 187

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

DRAFT COMMUNIQUÉ

1. We, the Home Affairs, Interior Security and Immigration Ministers of [redacted] have come together in London, United Kingdom on 29–30 July 2019. Guided by our shared responsibility and commitment to build a more peaceful and secure world for our citizens, we affirm our determination to promote our shared values and protect our nations from existing and emerging security threats whether faced in our communities, at our borders, or in the cyber space.

Cyber and Online Threats

1. An open, interoperable, reliable, and secure internet is fundamental to the social and economic development of communities across the globe. With it comes a responsibility to tackle the complex and evolving nature of those threats that seek to undermine its potential. We also reaffirm the norms, rules and principles for the responsible behaviour of states in cyberspace previously endorsed by the UN General Assembly in 2013 and 2015, and commit to continue to work to see these norms strengthened and implemented.

2. It is also vital that [redacted] partners support each other in ensuring coordinated and efficient responses to cyber threats, including incidents at a national and international level, and against different types of victims. We commit to continue to develop and share learning on cyber threats and responses in order to facilitate a collective improvement in both understanding and response capability across the five countries.

3. The nature of 5G, whilst bringing unparalleled opportunity will also increase the [redacted] risks to the integrity of our telecommunications networks. [redacted] There is agreement between the [redacted] Eyes of the need to ensure supply chains are trusted and reliable to protect our networks from unauthorised access or interference. [redacted]

Emerging Technologies

1. Emerging technology reflects the growth of increasingly autonomous, intelligent and connected devices that blur the distinctions between the physical and digital worlds. We recognise the importance of protecting our citizens and economies from threats whilst empowering them to engage with new technology. The security of the Internet of Things is a critical issue that requires international cooperation and harmonisation of standards to achieve the required effect across diverse markets.

2. It is essential that nations and their people can trust the technology that will underpin their societies now and in the future. Emerging technologies bring a range of opportunities and challenges, including for our approaches to cyber security. We recognise the importance of open, diverse, competitive and trusted critical technology markets, where security-by-design is a fundamental principle. Our nations [redacted] a joint Statement of Intent, which will align our approaches to enhancing the security of the Internet of Things devices, to provide better protection to users by advocating that devices should be secure by design. The Statement will [redacted] our nations to actively seek out opportunities to enhance trust and raise

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)



awareness of best practice associated with IoT devices and reaffirms the need to identify and engage likeminded nations to encourage international alignment on IoT security. We welcome complementary international efforts to improve the security of critical and emerging technologies.

3. In recent years unmanned aircraft systems, often referred to as 'drones', have rapidly evolved in terms of capability, availability, and uptake for commercial and recreational use. Drone technology has the potential to offer significant benefits to economies and quality of life. However, the malicious, unlawful or inadvertent misuse of drones can pose a risk to public safety, be deliberately used to facilitate or commit a wide range of criminal acts, and also present a threat to our national security. We commit to create a stronger approach to drones informed through co-ordinated and in-depth information sharing around threat, vulnerabilities and counter-drone technology. We will also enable the security community to identify what more could be done at the manufacturing stage to mitigate drone risk by design. Work to commence this will begin immediately and the UK will host a event at the Home Office Security and Policing Event in March 2020 to enhance cooperation.

Borders and Asylum

1. Facilitating the legitimate movement of people across our borders is essential to our economic prosperity. We acknowledge the importance of safe and regular immigration and protecting refugees and those seeking asylum and reaffirm the positive benefits that managed immigration, settlement and integration brings to our societies.

2. We recognise the need to modernise border security systems to deal with evolving threats. We therefore commit to pursue expanded data sharing on travellers prior to and at the border to facilitate the secure movement of legitimate goods and in ways that maintain privacy, data security, and are consistent with domestic law.

3. We reiterate the sovereign right of states to strong border management, including the responsibility to deter, prevent, detect and disrupt those who seek to evade or facilitate the evasion of border controls. We also recognise that our ability to deliver timely protection to those genuinely fleeing persecution is hampered by those who abuse or facilitate the abuse of our border and immigration systems, including our asylum systems. We therefore commit to increase our collaboration regarding such activity. We commit to cross-border information sharing on, but not limited to, travelling child sex offenders, in line with domestic legislation. We further reiterate our commitment to work together and with global partners to secure the efficient removal of individuals without lawful status in our countries.

Countering Foreign Interference - Election Security and Strengthening Democracy

1. Building on last year's commitment to establish a mechanism to share approaches to combating foreign interference — being the coercive, deceptive and clandestine activities of foreign governments, actors, and their proxies, to sow discord, manipulate public discourse, bias the development of policy, or disrupt markets for the purpose of undermining our nations and our allies— our countries have shared strategies that protect our electoral institutions and democratic processes from foreign interference and other hostile state activity. We commit to maintaining these efforts, and will continue our collaboration to combat foreign interference in other areas such as the economy and academia.

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



[redacted]

Joint Meeting of FCM and Quintet of Attorneys-General

1. On 30 July, Home Affairs Ministers and Attorneys General met together. We discussed countering child sexual exploitation and abuse, countering violent extremism and terrorism both online and offline, foreign terrorist fighters, and encryption.

Countering Online Child Sexual Exploitation and Abuse

1. We commit to support more effective prevention, disruption and investigative responses to this [redacted]
2. We commit to prioritise the sharing of technology, data and expertise between us to help tackle the global threat of online child sexual abuse, recognising the great benefits that would come from closer cooperation, especially as we explore technologies to respond to new threats such as the live streaming of child sexual abuse.
3. We reaffirm our commitment to the WePROTECT Global Alliance, a partnership of Member States, global technology companies and international and non-governmental organisations working together to end online child sexual exploitation and sexual abuse.

Use of the Internet for Terrorist and Violent Extremist Purposes

1. The internet must not be a safe haven for terrorist and violent extremist content and activity. At the same time, our efforts, including with digital industry, to combat terrorist and violent extremist purposes must be undertaken in a manner consistent with national and international law, including protections for human rights and fundamental freedoms.
2. To this end, we reaffirm our commitment to supporting academic and civil society research on all forms of terrorism and violent extremism, including on the challenges of defining and addressing terrorism and violent extremism, better understanding algorithmic confinement, and developing credible counter and alternative narratives.
3. We commit to continue to work with digital industry to establish protocols for emergency situations, as well as safeguards to protect news reporting.
4. We reaffirm our commitment to engage smaller platforms in addressing their exploitation by violent extremists and terrorists, developing and sharing ways to support their efforts to reduce

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



their exploitation and encouraging industry to work together to share understanding and build capacity to tackle the threat across all platforms.

5. We also commit to support increased information flows between digital industry and the [redacted] including by providing threat-related information to digital industry from the security, intelligence and law enforcement communities to better inform how they moderate content. To build our collective understanding, we also encourage companies to share more data and information about how terrorists exploit their services and their efforts to disrupt this with governments, law enforcement and civil society.
6. We commit to collaborate on progressing the important work that has been undertaken in other likeminded fora, such as the strengthening of the Global Internet Forum to Counter Terrorism and facilitating broad collaboration, drawing on as appropriate the goals of:
    a. The G20 Osaka Leaders' Statement on Preventing the Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism; and
    b. The Christchurch Call to Action.
7. We call on the Countering Violent Extremism Working Group to facilitate information and knowledge exchange on all forms of violent extremism and terrorism.

Online Safety and Encryption

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)



Foreign Terrorist Fighters

1. Whilst Da'esh has lost the territory of the so-called 'caliphate', as an international community we remain vigilant against terrorism and the continued threat posed by Foreign Terrorist Fighters (FTFs). Within Syria and Iraq, Da'esh has transitioned back to its covert insurgency roots. Some of its members continue to pose a threat both in the region and more widely, whilst others are detained and best efforts must be made to bring them to justice.

2. [redacted] must continue to take the lead in addressing the issue of FTFs effectively, both in our own countries, and providing appropriate support to those countries most affected. We commit to maintain the international focus on addressing both relocating FTFs, and those now in detention. We commit to:

   - Take steps to coordinate, deconflict and prioritise our respective capacity building overseas in third countries, including through effective use of multilateral organisations such as United Nations (UN), and the Global Counter Terrorism Forum (GCTF).

   - Support third countries to fully implement UN Security Council Resolution (UNSCR) 2396, including providing support to build capability to collect, process and analyse Advance Passenger Information (API) and Passenger Name Record (PNR) data, to collect and use biometric data, to develop terrorist watchlists and share watchlist information, and contribute to and use Interpol databases, with full respect for human rights and fundamental freedoms, for the purpose of preventing, detecting and investigating terrorist offenses and related travel.

   - Support the International Civil Aviation Organisation (ICAO) PNR Task Force to establish a global standard for the responsible use and protection of PNR data that can resolve conflicts of law that inhibit the international transfer and processing of PNR data, as well as to support the work of the UN to build Member States' capability to collect, process and analyse API and PNR data.

   - Work together to promote Battlefield Evidence best practice and guidelines to improve global standards for the collection and use of Battlefield Evidence in investigative and judicial processes, including the Guidelines on the collection, use and admissibility of military-collected information presently under development by the UN.

   - Share frameworks and tools between the [redacted] on managing residual risk.

[redacted]

Conclusion

1. We reaffirm today the critical importance of the five country partnership. Bound by our history of cooperation, united by our shared values, and strengthened by our enduring friendship, we pledge the commitments made today as we seek to share opportunities and address security challenges together.

s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

BRIEFING NOTE FOR THE MINISTER

ONLINE HARMS:

CHILD SEXUAL EXPLOITATION AND ABUSE

Strategic Objectives

- Strengthen Canada's position as a key ally in the international efforts to address the transnational nature of child sexual exploitation and abuse online.
- Reassert Canada's support to make digital industry more accountable in the fight against child sexual exploitation and abuse online.
- [redacted]

Key Messages

Canada's Approach to Combatting Online Child Sexual Exploitation and Abuse Online in the Context of Online Harms

- The sexual exploitation of children online continues to devastate too many Canadians, as well as youth and families around the globe, with serious and long lasting consequences.
- Canada is committed to working with partners – domestically and internationally - to combat this serious crime that continues to transcend borders.
- Canada's approach is anchored in the *National Strategy for the Protection of Children from Sexual Exploitation on the Internet*, which is designed to increase capacity to investigate and track down predators, enhance public awareness, and support research/innovation to address this issue.
- The Canadian Centre for Child Protection is a key partner in implementing this Strategy. With the support of federal funding, they developed Project Arachnid, a leading-edge technology that can crawl thousands of web pages a second, detect sexual abuse materials, notify providers and ultimately result in the removal of exploitative content.
- They also support victims and survivors such as Phoenix 11, a group of survivors of child sexual exploitation who want to increase public

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

awareness about the widespread issue of child sexual abuse and the lifelong impacts of its recording and distribution on the Internet.

- Despite technological advances such as Arachnid as well other artificial intelligence tools, online child sexual exploitation continues to proliferate at an alarming rate as more and more people become connected to the Internet and new technologies facilitate the easy, anonymous creation of, access to and sharing of child sexual abuse material.

- Canada recently announced further investments to better protect children from sexual exploitation online. This funding will support Canada's efforts to: raise awareness of this serious issue; reduce the stigma associated with reporting; increase Canada's ability to pursue and prosecute offenders; and work with digital industry to find new ways to combat the sexual exploitation of children online.

Engagement with Digital Industry

- Canada welcomes the engagement of digital industry on the issue of child sexual exploitation and abuse online.

- Canada supports further dialogue with the digital industry on the issue of global industry responsiveness toward the removal of child sexual exploitation images.

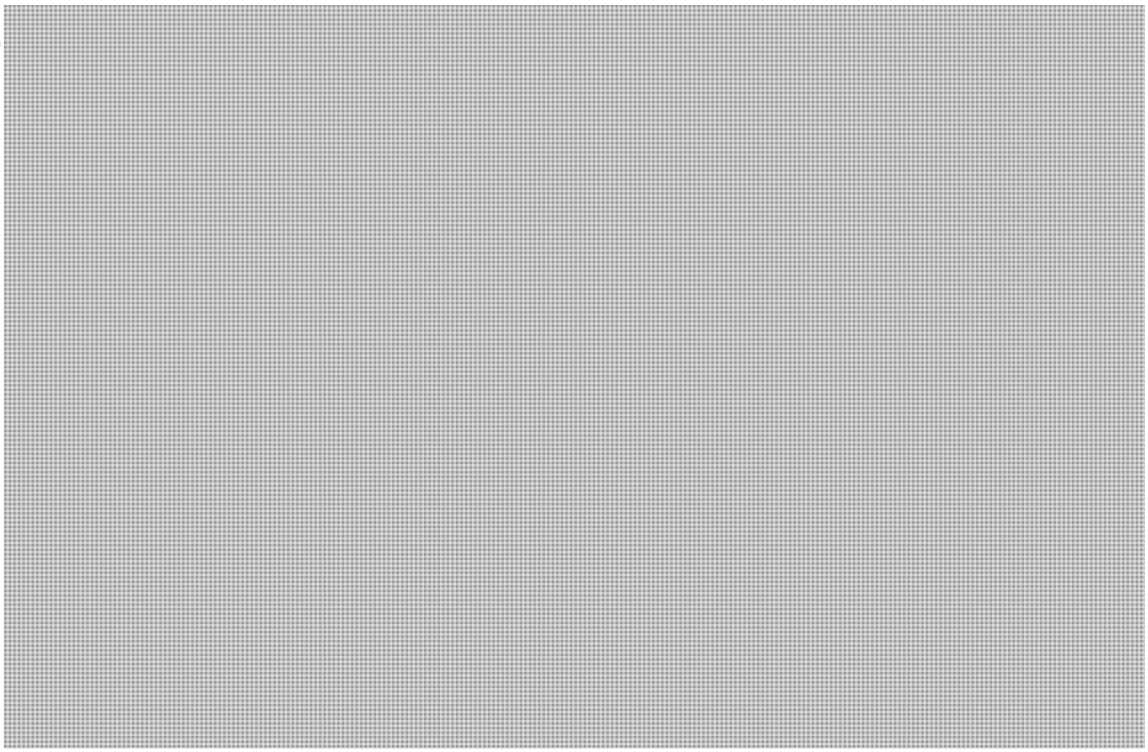
- Canada supports innovative approaches to addressing child sexual exploitation and working with partners, including digital industry, to develop technology-based solutions.

- Canada encourages Industry partners to work together, including with smaller companies, and share best practices to address online child sexual exploitation on their systems. Canada also encourages Industry to share good practices on prevention and education.

- Canada agrees that the digital industry, as a whole, should be guided by a set of voluntary guiding principles that provide a clear and consistent framework in the fight against child sexual exploitation and abuse and welcomes the progress made earlier today on the development of a set of "best practices" for the digital industry.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Data and Technology Sharing

- The sharing of information, tools and technology with Five Eyes partners will result in better prevention, identification, and prosecution of online child sexual offences.
- 
- Canada is supportive of enhanced information sharing related to investigational data, technological challenges, requirements and solutions; however there is a need to distinguish between data/technology and personal criminal information sharing which has many more legal considerations

Background

National Strategy for the Protection of Children from Sexual Exploitation on the Internet

The National Strategy for the Protection of Children from Sexual Exploitation on the Internet was launched in 2004. Public Safety Canada is the lead for the National Strategy and partners with the Royal Canadian Mounted Police, Justice Canada and the Canadian Centre for Child Protection (C3P), a not-for-profit organization responsible for operating Cybertip.ca, the national tip-line on the National Strategy. PS coordinates and oversees the implementation of the National Strategy, develops online CSE policy, and provides contribution funding to C3P for the operation of Cybertip.ca, as well as to other non-governmental organizations for targeted public awareness activities.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The National Strategy was renewed on an ongoing basis in 2009. That said, the technological landscape has changed considerably in recent years and technological advances have facilitated the easy, borderless access to, and sharing of, large quantities of images and videos of children being sexually exploited. In addition to the growing volume of child sexual abuse material online, technological advances have led to emerging new trends such as self-generated materials and sexting, sextortion, grooming and luring, live child sexual abuse streaming, and made-to-order content. The proliferation of online child sexual exploitation material demonstrates the need for the Government to continue to strengthen its response to this complex, escalating issue.

To this end, through It's Time: Canada's Strategy to Prevent and Address Gender-Based Violence (the GBV Strategy), Public Safety Canada received additional funding of $1.3 million annually, on an ongoing basis, in Budget 2017 to:

- Develop further public awareness;
- Enhance policy coordination and research; and,
- Enhance Cybertip.ca's capacity to support, through Project Arachnid, an increased rate of removal of child sexual abuse material online.

Budget 2018 announced further investment for the GBV Strategy of $5.8 million annually, on an ongoing basis, to enhance the RCMP's National Child Exploitation Coordination Centre's investigation capacity.

Building on investments in Budgets 2017 and 2018, Budget 2019 announced a further investment of $22.24 million over three years, starting 2019–20, to combat child sexual exploitation on the Internet. This funding will support Public Safety Canada's efforts to raise awareness of this serious issue, reduce the stigma associated with reporting, increase Canada's ability to pursue and prosecute offenders, and work together with industry to find new ways to combat this crime.

Initiatives funded through Budget 2019 will be rolled-out starting in the 2019-20 fiscal year, and will support a number of other Government priorities, including Canada's Strategy to Prevent and Address Gender-Based Violence.

Canadian Centre for Child Protection - Video presentation from Phoenix 11

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The Canadian Centre for Child Protection (C3P) is a not-for-profit organization responsible for operating Cybertip.ca, the national tip line. C3P receives $2.76 million per year (representing 76% of total project funding) from Public Safety Canada. This funding is to support the operation of Cybertip.ca as well as $857k per year for Project Arachnid, a web-crawling tool to identify child sexual abuse material online. C3P is actively engaged internationally to promote Project Arachnid with other governments. Funding also supports other C3P activities such as the production and dissemination of awareness and education materials and support to victims and survivors.

Phoenix 11 is a group of 11 survivors of child sexual exploitation supported by the C3P along with the National Centre for Missing and Exploited Children (NCMEC). The purpose of this group is to increase public awareness about the widespread issue of child sexual abuse and the lifelong impacts of its recording and distribution on the Internet. You met with the group in your office in Ottawa in November 2018. Lianna McDonald, the Executive Director of C3P, may attend the session to present the Phoenix 11 video, but this is to be confirmed.

FCM Engagement with Digital Industry

Online child sexual exploitation (CSE) is one of the most pressing public safety issues facing society today. Addressing this crime is a priority for Canada and for key allies, as reflected in the discussions at the 2018 FCM meeting in Australia. Digital industry representatives were invited to participate in a joint meeting with FCM ministers, however, none were able to attend. FCM ministers issued a joint statement which included a commitment to working with the digital industry to prevent online CSE, particularly live-streaming of child sexual abuse.

The digital industry Engagement Senior Official Group (DIESOG) was created to monitor and track digital industry progress related to the FCM statement on Countering the Illicit Use of Online Spaces. This includes close collaboration with digital industry to assess legal, policy and operational issues around the pro-active take-down by industry of Child Sexual Abuse Material (CSAM), and to further develop tools, technologies and techniques that could be used for this purpose and to reduce CSAM from being traded, distributed and shared. The Canada Centre for Community Engagement and Prevention of Violence at Public Safety Canada is the Canadian representative on DIESOG. The Serious and Organized Crime Division within Public Safety (PS), which leads the National Strategy for the Protection of Children from Sexual Exploitation on the Internet, sits on the Informal Working Group on Digital Engagement which supports Canada's participation in the DIESOG.

The Industry Roundtable meeting, preceding the Ministerial Roundtable on Online Harms, provides an opportunity to secure digital industry buy-in to work with Five Eyes countries to develop a set of voluntary principles to guide their role in addressing child sexual exploitation and abuse online. Continued engagement with the digital industry would be through DIESOG.

Data and Technology Sharing

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

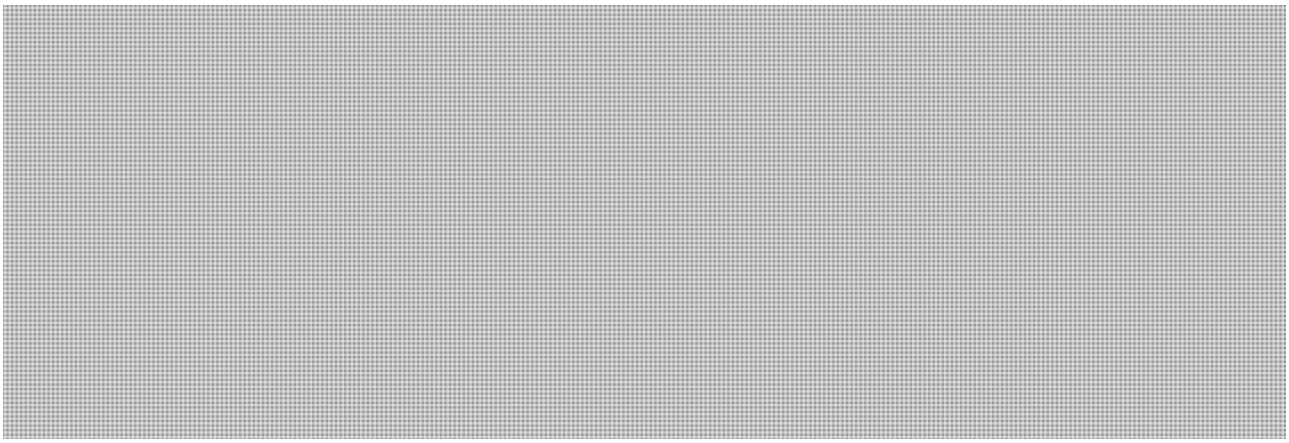
Data and technology sharing is seen as a crucial component of law enforcement's ability to address online child sexual exploitation and abuse internationally. There is vested interest on behalf of the Five Eyes partners to strengthen official information sharing mechanisms rather than creating new ones. Canada is supportive of enhanced information sharing related to investigational data, technological challenges, requirements and solutions; however there is a need to distinguish between technology and personal information sharing. Canadian privacy protection legislation and our constitutional framework require maintaining the case-by-case approach for personal information sharing. Discussions related to criminal information sharing are led by the Law Enforcement Information Policy and Strategy Group (LEIPSG) and should be kept separate from discussions on online child sexual exploitation and abuse.

Under the broader online harms category, terrorist use of the internet and child sexual exploitation and abuse have some similarities in terms of approaches and challenges to combat these crimes. These include: the role of the industry; legal considerations regarding privacy; issues related to takedown of material; as well as the need to develop artificial intelligence tools that can identify problematic behaviour online. However there are also key differences. Tools such as Project Arachnid and other automated tools currently facilitate the identification of child sexual exploitation and abuse material online.

Canadian law enforcement also participates in a variety of initiatives to promote technological innovation and to identify technical solutions, such as hackathons. In addition, the RCMP is one of the global leaders in developing artificial intelligence tools to increase capacity to prioritize and review, analyze and disseminate files more efficiently, as well as to improve the health and wellness of employees who examine high volumes of this data.

Use of Appropriate Terminology

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Drafted: CSCCB/LEBS/Mathilde Briere-Audet
Consulted: RCMP, JUS, PS's CCCEPV
Approved by: CSCCB/Burack

Pages 200 to / à 203

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

ONLINE HARMS:

TERRORISM AND VIOLENT EXTREMISM ONLINE AND OFFLINE

Strategic Objectives

- Highlight Canada's efforts to counter violent extremism and terrorism, including through the Canada Centre for Community Engagement and Prevention of Violence, and the need to work alongside the Five Eyes to focus on emerging trends and defining new forms of ideologically motivated violence;

- Underscore the need for coordinated Five Eyes engagement with digital industry, including the Global Internet Forum to Counter Terrorism (GIFCT), to counter violent extremism and terrorism in the online space; and,

- Emphasize initiatives recently announced by Canada such as $1M in funding for Tech against Terrorism to support smaller companies in their efforts to detect and remove content from their platforms; and a Youth Summit on Countering Violent Extremism Online in partnership with GIFCT companies.

Key Messages

- *You will co-lead this session with Minister Little of New Zealand. It is expected that Minister Little will speak first.* ***Your suggested opening remarks are attached separately; below are responsive key messages that you may wish to use during the open discussion.***

General

- Canada is deeply concerned by the threat posed by violent extremism and terrorism in all its forms.

- The principal terrorist threat facing Canada continues to be posed by individuals or groups inspired by Da'esh and al-Qaeda. However, Canada also faces threats from individuals espousing a variety of other ideological views, including white-supremacy and ultra-right wing nationalism.

Canada Centre for Community Engagement and Prevention of Violence

- The Canada Centre for Community Engagement and Prevention of Violence (Canada Centre) leads Canada's efforts to counter radicalization to violence in all its forms.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- In December 2018, the Canada Centre released the National Strategy on Countering Radicalization to Violence, which highlighted three priorities:
    - Building, sharing and using knowledge;
    - Addressing radicalization to violence in the online space; and
    - Supporting interventions.
- Additionally, the Canada Centre launched a National Expert Committee on Countering Radicalization to Violence. The Expert Committee provides guidance on implementing the three priorities of the National Strategy, and is comprised of representatives with a diverse range of backgrounds.

Recent Trends in Violent Extremism and Terrorism

- Canada is seized with the growing threat of violent extremism. Like many of our Five Eyes colleagues, Canada has felt the effects of this phenomenon.
- In 2017, Alexandre Bissonnette killed six and injured more at a mosque in Quebec City. He obsessively consumed online content which could be qualified as extreme far-right and anti-immigration.
- Alek Minassian, the alleged perpetrator of the Toronto van attack which killed 10 and injured 13 more in 2018, was immersed in the incel (involuntarily celibate) ideology, which promotes male supremacy and misogyny.
- Defining these types of violent extremist acts is challenging. Adherents often have limited interactions with formal networks and leadership structures. Grievances often depend on local social and political contexts.
- We do know that these types of incidents are growing, and represent a threat to national security and our collective security. While the manifestations can be local, these violent extremist movements are also globally interconnected.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.20(1)(c)
s.21(1)(a)

- Canada recently added, for the first time, two right-wing extremist groups with a presence both internationally and in Canada – Blood & Honour, and Combat 18 – to the *Criminal Code* list of terrorist entities. This will block the financing to such groups when they attempt to use Canada's financial system.

- We also know that violent extremism can involve hate speech and hate crime. In addition to the hate speech and hate propaganda provisions in its *Criminal Code,* Canada has taken several steps to address this by:

    - Investing in research and supporting programming that addresses violent right-wing extremism and hate in Canada to bolster the efforts of law enforcement, policy makers and community organizations;

    - Doubling investments in the Security Infrastructure Program to help Canadians protect themselves from hate-motivated crimes through enhancements to security infrastructure for places of worship, and community centres.

    - In Canada, the online environment is a major area of activity for violent extremists, including those that typically fall under the umbrella term of 'violent right-wing extremist.'

- These types of violent extremists operate primarily, though not exclusively, online, and are deliberate in how they skirt the line between hate speech and free speech. This activity may not breach platforms' terms of service or Canadian laws. Moreover, online hate can be communicated through media not typically counted in "speech," including images and video.

- Major digital industry players, [redacted] have taken steps against such actors and content. For example, [redacted]

- However, some platforms, [redacted] continue to host content willingly. Others, [redacted] have varying degrees of willingness to address the issue.

- As part of our efforts to be more effective in engaging these companies, it is therefore imperative for us to better define and identify the kinds of

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

complex threats we are facing, including through support for and sharing of research into the markers of threat and harm in the online space.

- It is also important to discuss how we can work together to engage those companies that are hosting the worst content and encourage their compliance with laws and norms surrounding hateful, violent extremist and terrorist content.

- Credible counter-narratives and alternative content can be effective for specific vulnerable audiences when well-targeted against violent extremist and terrorist content. They should be deployed to address all forms of violent extremism. Engaging youth and civil society in these efforts is critical to ensuring these efforts are effective and credible.

- Finally, it is important for Five Eyes countries to share best practices and information on the legal instruments against hate, and how these may be applied to combat all forms of violent extremism.

Violent Extremist and Terrorist Use of the Internet

- There are often real-world consequences to an individual's exposure or engagement with violent extremist and terrorist content online.

- In fact, the most recent violent extremist and terrorist attacks within the Five Eyes, including in Canada, have a nexus to the online space, where perpetrators were active in and influenced by online communities sharing and promoting violent extremist and terrorist messaging.

- There are a number of ongoing multilateral efforts to address violent extremist and terrorist use of the internet (VETUI), and together we can do more to leverage our strengths for collective benefit.

- First, we can expand our partnership on VETUI commitments stemming from the G7, G20 and Christchurch Call to Action. For example, we can continue to build on our respective efforts to work with digital industry to implement emergency protocols, support smaller companies, and invest in research.

- Second, we can further leverage our strengths. As an intelligence-sharing partnership, we can draw on our established links to better identify threat

s.15(1) - Int'l
s.20(1)(c)
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

activity online, inform our domestic efforts to engage with digital industry and regulate and legislate against VETUI, and share lessons learned.

- We can also use our strong relationships with digital industry to move beyond the "content removal" discussion. We know that there is more to content moderation than simply removal, which can push activity to the more hidden parts of the online space, as well as interfere with needs for situational awareness including during crisis situations.

- It is important for us to call on digital industry to work more collaboratively with law enforcement and legal authorities on the preservation of violent extremist and terrorist content that might be needed as evidence in investigations and trials, while at the same time ensuring this content is not publicly accessible.

- [redacted]

- It is also important for us to reiterate the need for accountability and transparency, particularly in terms of algorithmic confinement. Digital industry must use their tools and capabilities to ensure their algorithms are not directing platform users to violent extremist and terrorist content.

- This is particularly important for those platforms that lack capacity to address the threats to their platforms. Canada recently provided $1M in funding to Tech against Terrorism to provide that kind of support to smaller companies in their efforts to detect and remove terrorist content from their platforms.

- [redacted] These platforms host some of the most vile and harmful content on the internet and they cannot be allowed to provide a safe haven for violent extremists.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Finally, as strong democratic countries, we can leverage our collective experience to develop solutions that ensure the protection of fundamental human rights and freedoms in the pursuit of a safer internet.

Reforming the Global Internet Forum to Counter Terrorism

- [redacted]
- [redacted] Canada recommends that the DIESOG continue their work, focusing on areas of strength for the Five Eyes' partnership. Where appropriate, DIESOG should advance these efforts through forums such as the G7 and the Christchurch Call to Action, while continuing to engage bilaterally with key players.

- At the same time, Canada reiterates its preference for an expanded, more transparent and accountable GIFCT.

Legislative and Regulatory Options

- Canada continues to assess its available regulatory and legislative options for improving the safety and security of the online space, while protecting and promoting fundamental human rights and freedoms.

Background

Recent Trends in Violent Extremism and Terrorism

Canada Centre for Community Engagement and Prevention of Violence

In December 2018, the Canada Centre Community Engagement and Prevention of Violence (Canada Centre) launched the new *National Strategy on Countering Radicalization to Violence.* It outlines the Government of Canada's approach and key priorities in countering radicalization to violence. The three priorities are: (1) building, sharing and using knowledge; (2) countering radicalization to violence in the online space; and (3) supporting interventions.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

In January 2019, the Canada Centre also launched the National Expert Committee on Countering Radicalization to Violence. The Committee provides guidance to you, as the Minister of Public Safety and Emergency Preparedness, in implementing the three priorities of the National Strategy. The Committee's membership reflects a broad representation of backgrounds and expertise in the field.

Violent Right-Wing Extremism

Along with the *National Strategy on Countering Radicalization to Violence*, the 2018 *Public Terrorist Threat Report* notes that violent right-wing extremism as a growing threat in Canada and worldwide. Violent right-wing extremism has traditionally been driven by fear and hatred, and includes a range of individuals and groups, often in online communities, that back a wide range of issues and grievances, including: anti-government and anti-law enforcement sentiment, advocacy of white nationalism and racial separation, anti-Semitism and Islamophobia, anti-immigration, male supremacy, and homophobia.

Traditionally in Canada, violence linked to right-wing extremists has been sporadic and opportunistic. Additionally, violent right-wing extremism in Canada is found primarily in the online space. However, attacks perpetrated by individuals who hold violent right-wing extremist views and other lesser-known forms of ideological extremism can occur. A recent example is the April 2018 van attack in Toronto, Ontario, which resulted in the deaths of 10 people and alerted Canada to the dangers of the online Incel ("involuntarily celibate") movement. Another example is Alexandre Bissonnette who, on January 29, 2017, killed six and injured more at a mosque in Quebec City. He had used the platforms provided by mainstream digital industry to search for alt-right, conspiracy, and Neo-Nazi content.

Link to Hate Crime

The Canada Centre is prioritizing research into the links between hate crime and violent extremism. Hate crime in Canada has been measured by Statistics Canada since 2009 recording self-reported hate crimes, and hate crimes reported to law enforcement. Hate crime in Canada has risen each consecutive year since 2013. The 2017 Statistics Canada reporting found an increase of 47% in police-reported hate crimes since 2016 – the highest level since comparable data began in 2009. The main targets for hate crime are Muslim, Jewish and black communities. In 2017, the United Nations Committee on the Elimination of Racial Discrimination recommended Canada improve its approach.

Violent Extremist and Terrorist Use of the Internet

The Canada Centre leads the Government of Canada's efforts in preventing and countering violent extremist and terrorist use of the internet (VETUI). Canada is taking a number of steps to actively combat this issue, including domestic and international efforts.

The Department of Justice leads the Government of Canada in developing criminal law. The *Criminal Code* has hate crime and hate propaganda provisions, including the ability of a judge to order the deletion of hate propaganda made publicly available through a computer system in the jurisdiction of the court. There is also a wide range of terrorism offences, and counselling or

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

inciting any of these offences gives rise to criminal liability. Finally, the recently enacted *National Security Act, 2017* created a new counselling offence of counselling a terrorism offence without identifying a specific terrorism offence. The offence may be committed whether or not a terrorism offence is committed by the person who is counselled. There is also the ability of a judge to order the deletion of terrorist propaganda made publicly available through a computer system in the jurisdiction of the court.

Domestic efforts:

The Community Resilience Fund is supporting research and projects focused on better understanding and providing solutions to address VETUI, including:

- *Updating the Environmental Scan of Right Wing Extremism in Canada*: the University of Ontario Institute of Technology is establishing an updated, comprehensive view of the beliefs, motivations, activities and connections that characterize the right-wing extremism movement in Canada, and will include an analysis of online content and media coverage led by the UK's Institute for Strategic Dialogue.

- *Pushing Back Against Hate in Online Communities*: MediaSmarts examined the attitudes and experiences of 1000 young Canadians towards online hate speech and violent radicalization. Findings were recently published and included recommendations such as setting clear rules for platforms' community standards, and making it easier to report hate.

- *Canada Redirect*: Moonshot CVE is providing positive content to vulnerable individuals searching for violent extremist material online. The technique known as the "Redirect Method," uses online advertising tools and internet video channels to direct individuals to content created by credible third parties that challenge ideologies that can motivate destructive behaviour and attitudes.

International and multilateral efforts

Canada regularly engages in multilateral meetings and processes on countering VETUI. The 2019 G7 Interior Ministers' Meeting culminated in an outcome document, "Combating the use of the internet for terrorist and violent extremist purposes." In addition to reiterating commitments from the 2018 Security Ministers' Meeting, ministers called on digital industry to establish emergency protocols for content moderation during emergencies; and, provide support to small online platforms to detect and remove content.

Canada also recently participated in the Christchurch Call to Action Summit on May 15, 2019, hosted by New Zealand Prime Minister Ardern, and French President Macron on May. The Christchurch Call was signed by eight digital industry platforms and 17 countries, and committed both governments and digital industry to improve their work on combating VETUI, including joint efforts.

s.15(1) - Int'l
s.20(1)(c)
s.21(1)(a)
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Digital industry engagement

Canada regularly engages with digital industry, primarily the member companies of GIFCT, which includes Facebook, Google, Microsoft and Twitter.

In October 2018, Facebook co-hosted an event with the Canada Centre, with brought 50 youth to Facebook's Toronto headquarters to learn about developing online counter-narratives. Canada is planning a Youth Summit on Countering Violent Extremism Online in the near future in partnership with GIFCT companies.

[redacted]

The Canada Centre is also expanding its relationships with other platforms, and has held introductory meetings with Amazon, Apple, DropBox and CloudFlare.

Key issues with digital industry

[redacted]

1. Transparency in Algorithmic Confinement

An ongoing issue is the lack of transparency from digital industry on how they are addressing this issue, particularly related to algorithmic confinement. Both the G7 and FCM have called on digital industry to be more proactive and open with government about their efforts to combat violent extremist and terrorist use of the internet, including transparency regarding their algorithms and how they may be used to direct individuals to violent extremist and terrorist content, and to strengthen their engagement with civil society.

2. Engaging Smaller Platforms

s.13(1)(a)
s.15(1) - Int'l
s.20(1)(c)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Although there is some success from the mainstream platforms to remove extremist content, much of it has been in the area of al-Qaeda or Da'esh inspired content. Removing hate-motivated speech is more complex and challenging, in light of constitutionally protected provision of freedom of expression.

As the large technology companies increase efforts to remove harmful content, violent extremists and terrorist are increasingly moving to smaller platforms,

Legislative and regulatory options

Violent Extremist and Terrorist Use of the Internet

Two of the Five Eyes, Australia and the UK, have taken steps towards legislation. Australia introduced new legislation in early April 2019, which calls for digital industry to proactively and expeditiously remove illicit content from their platforms, and imposes harsh penalties, including potential jail sentences, on digital industry executives who fail to do so.

Also in early April 2019, the UK released a White Paper on Online Harms, which proposed the establishment of a new duty of care on digital industry to increhse their responsibly for harmful content on their platforms, and a regulatory body to oversee, implement and enforce new regulations.

The DIESOG is mandated with coordinating Five Eyes engagement with digital industry to ensure a coordinated approach.

Drafted: PACB/Canada Centre/Emily Nickel
Consulted: PS/Canada Centre, NSOD, CSIS, RCMP, Justice
Approved by: PACB/ Wherrett

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Five Country Ministerial 2019

Session 8: Terrorism and Violent Extremism Online and Offline

Remarks

for

The Honourable Ralph Goodale

Minister of Public Safety and Emergency Preparedness

Tuesday, July 30, 2019

London, United Kingdom

Word count for remarks: 912 (8 minutes @ 120wpm)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- **You will be providing opening remarks with New Zealand's Interior Minister, Andrew Little**

- ***First remarks to be provided by Minister Little***

- Thank you, Minister Little, for your remarks on the Christchurch Call to Action, and for highlighting New Zealand's efforts to combat violent extremist and terrorist use of the internet in the wake of the horrific terrorist attack on March 15, 2019.

Violent Extremist and Terrorist Use of the Internet

- In Canada, the online environment is a major area of activity for violent extremists.

- And there are often real-world consequences to an individual's exposure to or engagement with violent extremist and terrorist content online.

- In fact, the most recent violent extremist and terrorist attacks within the Five Eyes, including in Canada, have had a nexus to the online space,

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

where the perpetrators were active in and influenced by online communities promoting violent extremist and terrorist messaging.

- While the horrific events that took place in Christchurch coalesced global support for addressing violent extremist and terrorist use of the internet – including from digital industry – we know that there is still much work to be done.

[redacted]

- At the national level, Canada is making progress with a number of digital industry partners, including those in the Global Internet Forum to Counter Terrorism.

- For example, [redacted] we co-hosted an event with Google that brought together academics, civil society, frontline

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

practitioners, and government officials to hear from Google's Trust & Safety team about their approach to content moderation.

- Canada also recently announced funding of up to $1 million for Tech Against Terrorism, an organization affiliated with the UN Counter Terrorism Executive Directorate, to help them support smaller companies in fighting the exploitation of their platforms by violent extremists and terrorists.

- These initiatives highlight that preventing and countering violent extremist and terrorist use of the internet requires close collaboration with civil society, academia and digital industry.

Violent Right-Wing Extremism

- Canada is seized with the growing threat of violent extremism, including violent right-wing extremism. We have not been immune from the senseless violence caused by radicalized individuals.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- For example, in 2017, Alexandre Bissonnette killed six and injured more at a mosque in Quebec City.

- Alek Minassian, the alleged perpetrator of the Toronto van attack which killed 10 and injured 13 more in 2018, was immersed in the involuntarily celibate or 'incel' ideology online, which promotes male supremacy and misogyny.

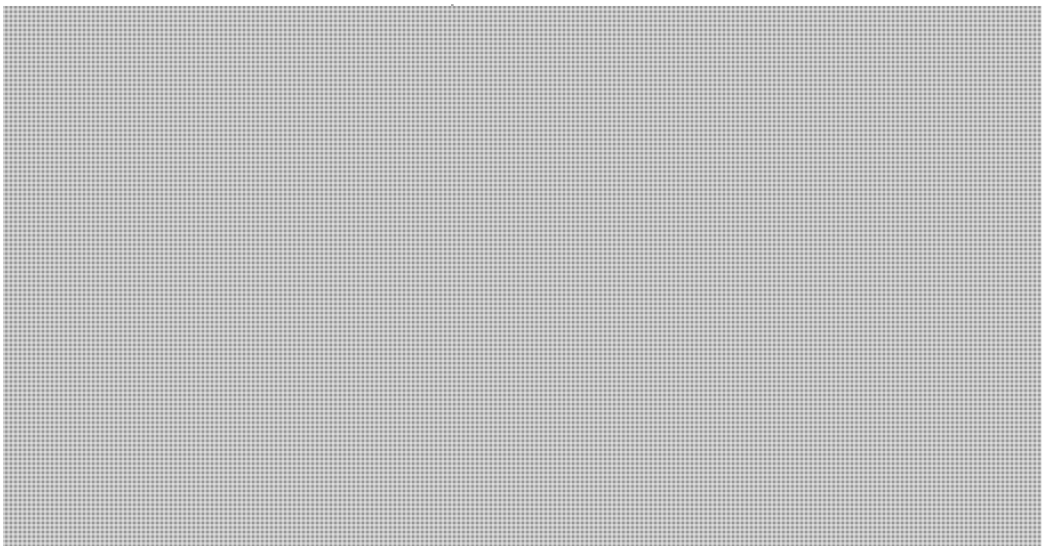
- We know that incidences of violent right-wing extremism are not unique to Canada, and represent a threat to our national and collective securities.

- Canada judges that the global violent right-wing extremist threat will increase as the sources of inspiration and grievances continue to impact the milieu.

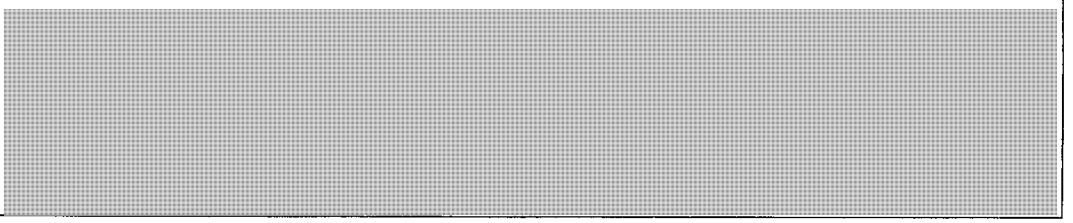
- And we are responding to this threat. For example, Canada recently added two violent right-wing extremist groups – Blood & Honour and Combat 18 – to our designated list of terrorist entities for the first time.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- We also know that violent right-wing extremism often has a nexus to hate speech and hate crime. In addition to our existing criminal provisions on hate speech and propaganda, Canada is investing in research and programming to address hate, and increasing our funding for security infrastructure that protects Canadians from hate-motivated crimes.



- In conclusion, I would like to thank both my interior ministry colleagues and those from our justice departments for their interest in this topic.



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

	[redacted] • I look forward to a productive discussion. Thank you.

Pages 221 to / à 226

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

s.16(1)(b)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

BRIEFING NOTE FOR THE MINISTER

ENCRYPTION

Strategic Objectives

- Reassert Canada's unwavering support to finding common solutions with Five Eyes partners [redacted]
- Exchange perspectives on the effectiveness of different laws and policies [redacted]
- Confirm Canada's active engagement to safeguard encryption and mitigate its challenges in collaboration with industry.

[redacted]

Key Messages

Encryption

Safeguarding Encryption and Gaining Public Support

- [redacted] it is also in Canada's interest that encryption technologies remain robust and widely-used in order to safeguard cybersecurity and the digital economy.
- Further action on encryption in Canada will only be possible to the extent that we can reassure Canadians that we do not intend to undermine the security of the communications products and services that they use.

Way Forward

- [redacted]

s.15(1)
s.15(1)(d)(ii)
s.15(1)(g)
s.16(1)(b)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Canada is supportive of deepening collaboration between investigative agencies and service providers. Our priority is building stronger relationships with industry. We believe that progress can be made if governments are kept informed when decisions regarding new products and services are made.

- We believe investigators would have more success in seeking communication service providers' assistance if governments affirm that we do not seek to undermine the security of communications services or restrict the spread of in-demand encryption technologies.

[redacted]

[redacted]

Threat assessment

[redacted]

s.15(1)(d)(ii)
s.15(1)(g)
s.16(1)(b)
s.21(1)(c)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Bilateral engagement

- We are fully in support of coordination among the Five Eyes to find solutions and strategies in approaching the private sector as a united group to discuss how they can support us in light of the diminishing access to the content of communications.

[redacted]

- While we should have a dialogue with the company on the impact of end-to-end encryption on public safety, we should keep in mind that it is a valid and understandable decision for a company to make.

Influence on the decision

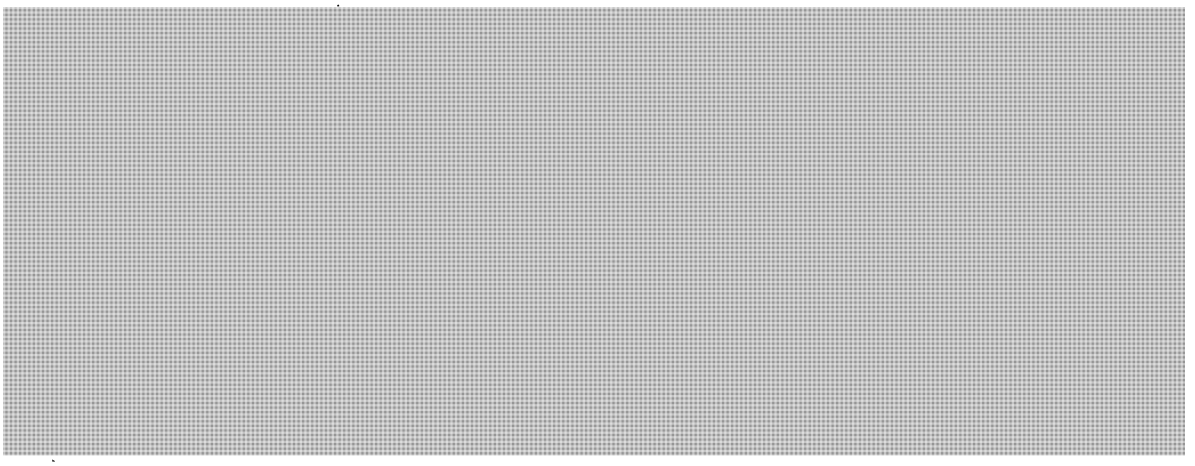
[redacted]

- Any convincing alternatives that we propose will need to take into consideration the perception of the public as this may be an essential factor.

- We believe it may be more fruitful to focus on the difficulties for law enforcement and on possible solutions, while avoiding branding end-to-end encryption itself as a threat or a negative development.

s.15(1)
s.15(1)(d)(ii)
s.15(1)(g)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Privacy and Digital Charter

- As we go forward with consulting the industry on encryption, we should keep in mind the competing pressure on tech companies as to their privacy protections. For instance, Canada's government has recently released a Digital Charter, that underlines the importance of privacy, and Canada's Privacy Commissioner is currently engaged in litigation with Facebook in relation to the need for enhancing privacy protection.

- The launch of the Digital Charter was accompanied by a set of proposals to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal private sector privacy legislation. The Charter's principles provide a set of shared national priorities where citizens have confidence that their data and privacy is protected.

- Notably, the Digital Charter enshrine the principle that Canadians will have control over what data they are sharing, who is using their personal data, and for what purposes, and know that their privacy is protected.

- Going forward, privacy and cybersecurity will increasingly be key concerns for the public as the volume of sensitive and personal data stored online and in electronic devices rises.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Background

2018 Statement of Principles on Access to Evidence and Encryption

As part of last year Five Country Ministerial meeting, the Five Eyes released a Statement of Principles on Access to Evidence and Encryption. The statement stressed the importance of encryption to cybersecurity, [redacted] The need to cooperate with providers of information and communications technology and services was emphasised. Finally, the statement underscored the importance of the rule of law and due process, as well as the freedom of choice for Five Eyes countries to address encryption as they see fit.

The Statement of Principles garnered some media attention, and some criticism. The particular focus of criticism and comments was on what was characterized as a threat made by the five Governments; which was that if service providers did not voluntarily assist in providing unencrypted data, that Governments retain the right to proposed "technological, enforcement, legislative or other measures to achieve lawful access solutions".

Facebook privacy first platform

Earlier this year, Mark Zuckerberg announced proposals to make Facebook a "privacy first platform", principally by moving their three core messaging services (Facebook Messenger, Instagram Direct Messaging and WhatsApp) to a single, end-to-end encrypted environment. The justification for doing so has been built on an analogy that Facebook has enabled people to connect in the "digital equivalent of a town square" but that users increasingly want to be connected privately in the "digital equivalent of a living room". [redacted] As part of their announcement, Facebook committed to engage Governments on these proposals to discuss how to maintain user safety across their platform.

[redacted]

Existing end-to-end encrypted messenger programs such as WhatsApp or Telegram are already widely exploited by offenders to commit online child sexual exploitation offences, such as luring and grooming children or distributing child sexual exploitation material, in virtual anonymity. This would undoubtedly be magnified with the multi-billion users on Facebook and Instagram messenger platforms, which contrary to the aforementioned programs, are heavily used by youth.

s.15(1)
s.15(1) - Subv
s.15(1)(d)(ii)
s.16(1)(b)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Existing Solution

[redacted]

Public debate and stakeholders' engagement

While CSPs are receptive to engaging on encryption, they have strongly opposed attempts by governments to mandate access to encrypted data in ways that would undermine the security of their products or jeopardize the trust of their users. When faced with coercive government actions, CSPs have not hesitated to challenge them in court. For example, the associations representing major US CSPs filed amicus briefs in support of Apple during 2016 litigation over access to a dead terrorist's encrypted iPhone. Given the importance of protection of cybersecurity, these concerns would need to be fully addressed by any government policy that attempts to assist law enforcement with the challenge of encryption, both from a substantive perspective, and from a communications perspective.

Another challenge in this respect is that even if the requirements imposed do not in fact inherently weaken the protection provided by encryption, concerns regarding this possibility will likely continue to strongly influence the views of the public and stakeholders, and raise significant privacy concerns.

Drafted: NCSB/NSPD/[redacted]
Consulted: RCMP/CSIS/Justice
Approved by: NCSB/NSPD/Davies

Pages 233 to / à 239

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED
SOLICITOR-CLIENT PRIVILEGE

s.13(1)(a)
s.15(1) - Def
s.15(1) - Int'l
s.21(1)(a)

BRIEFING NOTE FOR THE MINISTER

FOREIGN TERRORIST FIGHTERS:

BATTLEFIELD EVIDENCE

Strategic Objectives

Key Messages

- Canada's first and preferred course of action with respect to returning FTFs is arrest and prosecution. When sufficient evidence exists, Canada will pursue charges and prosecute FTFs to the full extent of the law.

- The use of battlefield evidence is a very complex legal and operational issue, which is being examined by numerous Canadian departments and agencies.

- Canada sees great utility in sharing best practices and comparing approaches on this issue,

[1] Background information on Canadian FTFs and the Government of Canada's approach to addressing this issue is attached (**ANNEX A**)

RDIMS # 3093556

s.13(1)(a)
s.15(1) - Def
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

I. BATTLEFIELD EVIDENCE

Background

United Nations Security Council Resolution (UNSCR) 2396 underscores the importance of criminal justice tools in combatting terrorism. The resolution emphasizes the obligation of UN Member States, set forth in UNSCR 1373, "to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in support of terrorist acts *is brought to justice*." UNSCR 2396 stresses that Member States have the primary responsibility in countering terrorist acts. This responsibility necessarily includes the investigation, prosecution, and adjudication of their citizens for terrorism related crimes, as reflected in *inter alia*, UNSCR 2396's urging of Member States to develop and implement appropriate investigative and prosecutorial strategies regarding those suspected of committing foreign terrorist fighter-related offenses described in UNSCR 2178's paragraph 6.

While arrest and prosecution of FTFs is the Government's main priority, Canada and its allies face significant challenges in their attempts to obtain admissible evidence that can be used to help prosecute and secure convictions of terrorist suspects in judicial proceedings.

[redacted]

When authorized, the Department of National Defence (DND)/CAF may retain and analyze captured enemy equipment and material resulting from a CAF operation overseas. Information gathered abroad by CAF or international partners may be shared with Canadian intelligence agencies and/or law enforcement agencies in accordance with applicable laws. The ability to share with non-traditional interlocutors is a key issue. Information must be collected, handled, and processed to satisfy the admissibility requirements for legal evidence, and ensure that post-collection chains of custody adhere to the highest evidentiary standards.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.15(1) - Int'l
s.21(1)(a)

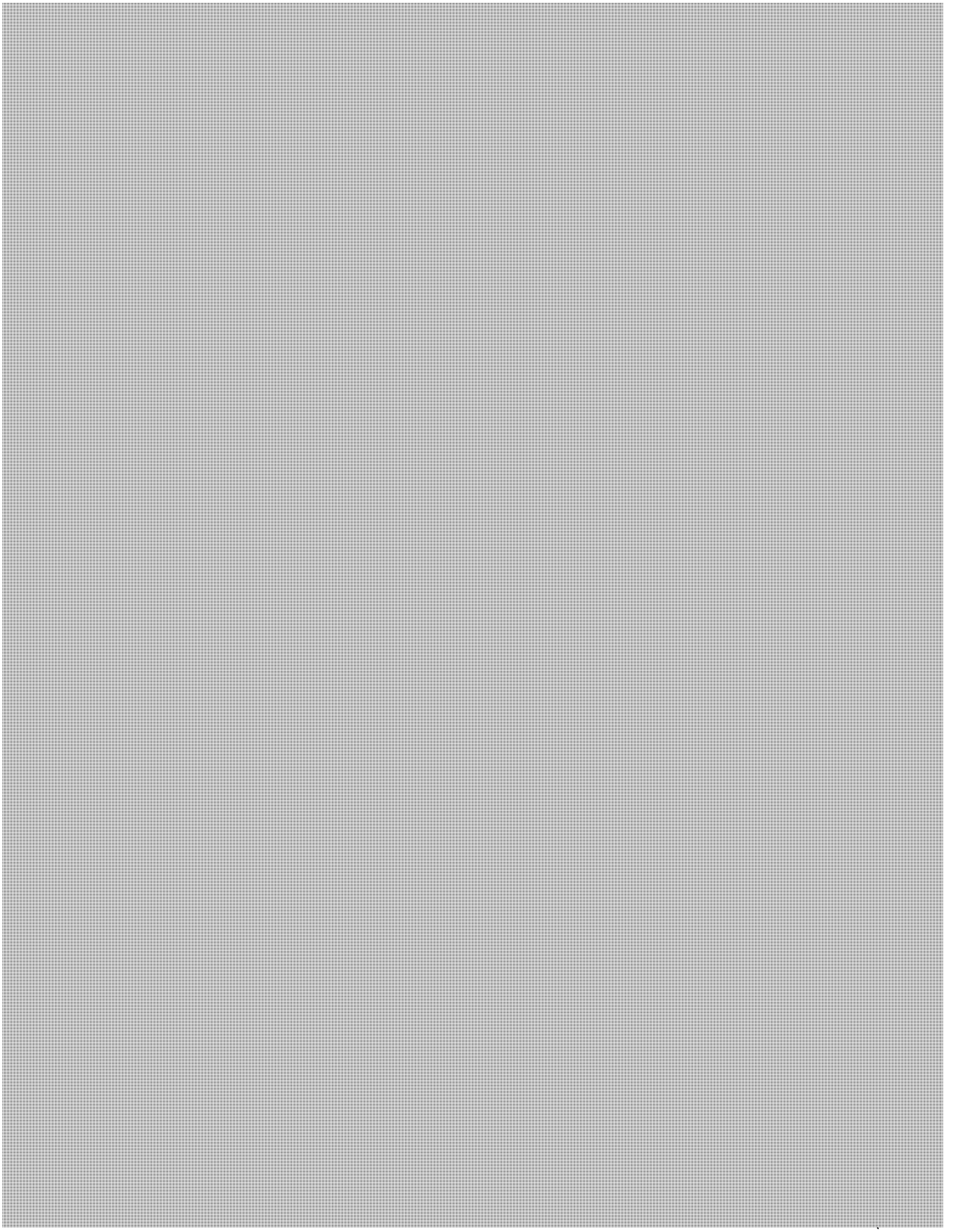
Notwithstanding some of the challenges related to collecting and securing battlefield evidence, a number of factors may help to maintain the integrity of the evidence, including the training and tasking of specialists, and/or by embedding law enforcement agencies with CAF in theatre. Moreover, capacity building in partner nations may help to increase awareness of other nations' specific legal admissibility requirements to help ensure that the evidence collected is not tainted.

To that end, in September 2017, the US Department of State (DOS), Department of Justice (DOJ), and Department of Defense (DOD) launched a battlefield evidence initiative to assist partner nations in using battlefield evidence effectively in civilian criminal justice proceedings. Based on the key issues and themes highlighted during these discussions, DOS, DOJ, and DOD collectively developed fourteen non-binding guiding principles.[2]

[2] A summary of the guiding principles is attached (**ANNEX B**)

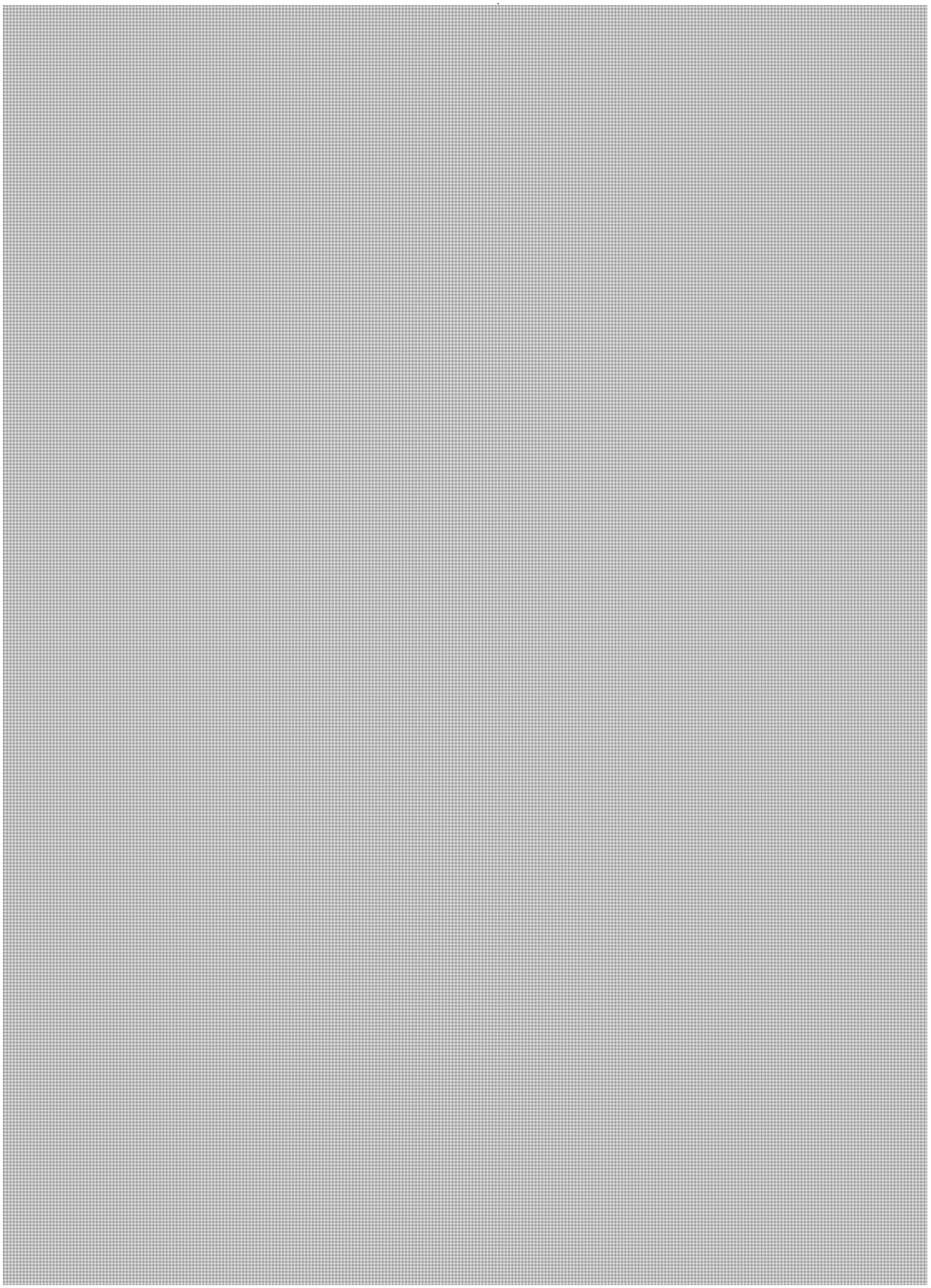
s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



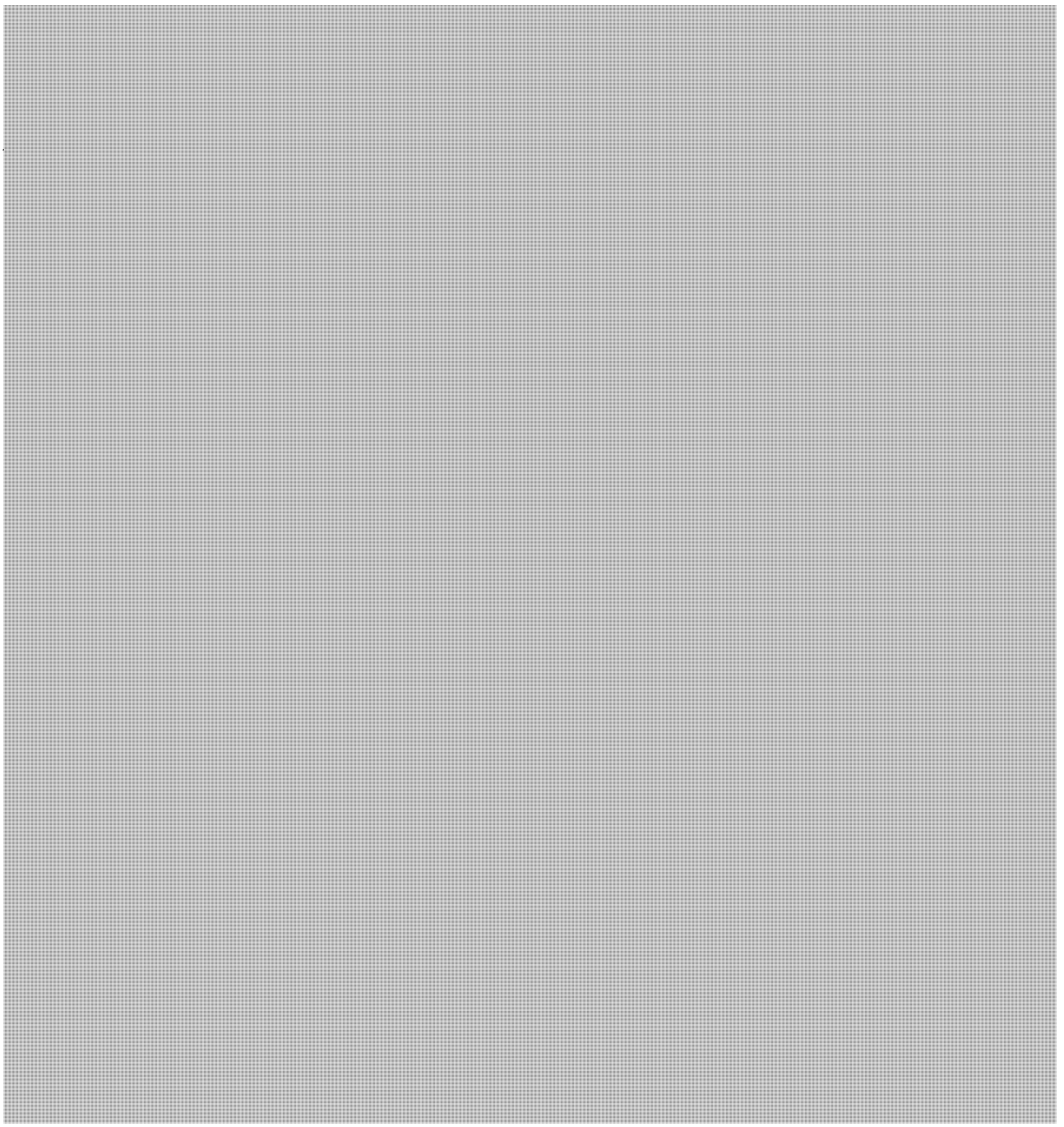
s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



s.13(1)(a)
s.15(1) - Int'l
s.15(1) - Subv
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Drafted: NCSB/NSPD
Consulted: DOJ, GAC, PPSC, RCMP, DND, NSOD
Approved by: NCSB/Beauregard

RDIMS # 3093556

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

ANNEX A: FOREIGN TERRORIST FIGHTERS

Background

Though FTFs are not a new phenomenon, Daesh was able to attract individuals in unpreceded numbers – over 40,000 from more than 110 countries. According to the *2018 Public Threat Report on the Terrorist Threat to Canada*, there are currently just over 190 individuals with a nexus to Canada who are abroad, including in Iraq and Syria. Just over 60 individuals have returned to Canada. Those numbers have remained relatively stable over the past three years, as it has become more difficult for extremists to successfully leave or return to Canada.

Specific offences with respect to terrorism were created in the *Criminal Code* following the 9/11 attacks of 2001. As of June 2019, a total of 56 individuals have been charged with terrorism offences over the years, and 29 of them have been convicted thus far. In 2013, offences specifically related to leaving or attempting to leave Canada for the purposes of committing certain terrorism offences were enacted in the *Criminal Code*. Since then, a total of 12 individuals have been charged with specific terrorism travel offences:

- five (5) have been convicted;
- two (2) have been acquitted;
- four (4) have outstanding warrants; and
- one (1) has had charges withdrawn

Government of Canada Approach

International

- The Five Country Ministerial process – established in 2013 – provides a forum for Canada, the United States (US), the United Kingdom (UK), Australia and New Zealand to discuss a range of common national security issues and identify areas for collaboration. Most recently, at the August 2018 meeting in Australia, Canada agreed with its partners to expand information sharing about known or suspected terrorists.

- Canada also a member of the Global Coalition to Counter Daesh, participating in both its civilian and military lines of effort to cut off Daesh's access to financing, stem the flow of FTFs, counter its propaganda, and engage in security and stabilization efforts. The Coalition was established in September 2014 and is composed of 73 members (including the UN, the European Union, INTERPOL and NATO). Canada is actively engaged in the Coalition's Working Group on Foreign Terrorist Fighters. The working group helps countries to implement UN Security Council Resolution 2178 and good practices identified by the Global Counterterrorism Forum.

- Canada also participates in the G7 Roma-Lyon Group, the G7 Experts Group on Transnational Organized Crime and Terrorism, and supports the G7 *Action Plan on Countering Terrorism and Violent Extremism*, where it has highlighted the importance of integrating gender considerations and the women peace and security agenda.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Domestic

- In 2014, the RCMP established the National Security Joint Operations Centre (NSJOC) to enhance the Government of Canada's response to "high-risk" travellers who pose a threat of terrorism-related violence in Canada and abroad. The NSJOC is an example of interdepartmental collaboration with several key partner agencies that facilitates real-time information exchanges and supports the coordination of operational responses. Participating agencies include the CBSA, CSIS, and Immigration, Refugees and Citizenship Canada.

- The Government of Canada manages the risk of returning FTFs through an interdepartmental committee on managed returns and the NSJOC. The RCMP is also proactively working with Canada's diplomatic missions overseas to identify returning FTF before they attempt to return to Canada.

- Once the RCMP is made aware of a possible returnee, they exchange information through the NSJOC and existing mechanisms to make an assessment of what risk they may pose. The interdepartmental committee on managed returns then meets to discuss what measures can be taken to control the return of the individual.

- In 2015, amendments to the *Secure Air Travel Act* enhanced the mandate of the Passenger Protect Program to not only mitigate threats to transportation security, but also prevent air travel for the purpose of engaging in terrorist-related activities.

- Also in 2015, the *Canadian Passport Order* was amended, providing the Minister of Public Safety and Emergency Preparedness the authority to cancel, refuse, or revoke a passport to prevent the travel of those seeking to engage in terrorist activity abroad, or other activities that may threaten national security.

Options Once in Canada

- Once in Canada, the Government has a number of tools to investigate and respond to returnees, including ongoing risk assessment for as long as necessary after an individual returns.

- The RCMP is focused on mitigating the threat posed by those engaging in terrorist activity and conducting criminal investigations with a view to supporting prosecutions.

- If there is insufficient evidence for a charge, the RCMP and its law enforcement partners continue their efforts to collect the necessary evidence to pursue charges.

- The RCMP also uses peace bonds to mitigate the threat an individual may pose.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Canada's law enforcement and security departments and agencies can also employ investigative techniques, including active physical surveillance and undercover operations, as well measures to reduce threats.

- Additionally, the Government has a number of administrative tools, like the Passenger Protect Program, passport cancellations/refusals/revocations and immigration action, if applicable.

- Countering radicalization to violence (CRV) efforts are also key to Canada's response to returnees, as demonstrated by community engagement by the RCMP, as well as the Canada Centre for Community Engagement and Prevention of Violence (the Canada Centre), which provides leadership and coordination on Canada's approach to CRV.

- The Canada Centre supports intervention programs that are equipped to handle a range of cases, including individuals who have travelled abroad to engage in terrorist activities. The interventions are led by health or social service professionals who address the needs and vulnerabilities of the individual.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

ANNEX B: SUMMARY OF THE 14 GUIDING PRINCIPLES FOR BATTLEFIELD EVIDENCE

• Ensure clear legal authorities and practices for military operations exist that allow for the collection and use of information.
• Develop legal frameworks that allow for the admissibility of battlefield evidence, including protection of classified information, as well as sharing information with non-military actors.
• Develop clear guidelines or policies addressing the security classification of battlefield evidence and its ability to be unclassified, where possible.
• Develop policies and procedures for the creation and maintenance of a chain of custody and the integrity of the information and/or materials as a way to ensure authentication.
• Create a systematic process to preserve information and objects that are collected and/or obtained by military personnel so that they are accessible and useable over the long term.
• Exploit military collected or obtained information and materials for identifying data.
• Establish processes for reviewing and downgrading the classification of information collected or obtained through military operations.
• Recognize that battlefield evidence can have a multitude of civilian counterterrorism-related uses.
• Use multilateral and/or regional platforms to share battlefield evidence with partner nations.
• Educate relevant government officials, particularly in the military, on the value of criminal prosecution.
• Conduct joint trainings, as appropriate, that includes military and law enforcement officers.
• Provide training to key interlocutors, such as judges and investigating magistrates, on the unique nature of battlefield evidence and the nature of the environment in which the military collects and obtains information and materials.
• Improve policymakers and practitioners' understanding that battlefield evidence will often require the need to develop independent, corroborating evidence.
• Advance the basic knowledge, understanding, and training of designated military forces to handle battlefield evidence.

Pages 250 to / à 251

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Int'l, 16(1)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 252 to / à 254

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

GAC APPROVED MEDIA LINES – JACK LETTS

- It is a Criminal Code offence to travel abroad to engage in terrorist activity. Where Canadian authorities have evidence that someone has engaged in terrorism, that person can expect to face the full force of the law.

- The Government continues to monitor and respond to the threat of extremist travellers who are suspected of travelling abroad to, join, support or engage with terrorist organizations. Canada takes the threats posed by these people extremely seriously.

- The Government of Canada is aware of Canadian citizens detained in Syria.

- Due to provisions of the Privacy Act, no further information can be disclosed.

Background context:

- [redacted]

- Given the security situation on the ground, the Government of Canada's ability to provide consular assistance in any part of Syria is extremely limited.

[redacted]

-

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FIVE COUNTRY
MINISTERIAL



Emerging Threats
London 2019

DRAFT COMMUNIQUÉ

1. We, the Home Affairs, Interior Security and Immigration Ministers of [redacted] have come together in London, United Kingdom on 29–30 July 2019. Guided by our shared responsibility and commitment to build a more peaceful and secure world for our citizens, we affirm our determination to promote our shared values and protect our nations from existing and emerging security threats whether faced in our communities, at our borders, or in the cyber space.

Cyber and Online Threats

1. An open, interoperable, reliable, and secure internet is fundamental to the social and economic development of communities across the globe. With it comes a responsibility to tackle the complex and evolving nature of those threats that seek to undermine its potential. We also reaffirm the norms, rules and principles for the responsible behaviour of states in cyberspace previously endorsed by the UN General Assembly in 2013 and 2015, and commit to continue to work to see these norms strengthened and implemented.

2. It is also vital that [redacted] partners support each other in ensuring coordinated and efficient responses to cyber threats, including incidents at a national and international level, and against different types of victims. We commit to continue to develop and share learning on cyber threats and responses in order to facilitate a collective improvement in both understanding and response capability across the five countries.

3. The nature of 5G, whilst bringing unparalleled opportunity will also increase the [redacted] risks to the integrity of our telecommunications networks. [redacted] There is agreement between the [redacted] of the need to ensure supply chains are trusted and reliable to protect our networks from unauthorised access or interference. [redacted]

Emerging Technologies

1. Emerging technology reflects the growth of increasingly autonomous, intelligent and connected devices that blur the distinctions between the physical and digital worlds. We recognise the importance of protecting our citizens and economies from threats whilst empowering them to engage with new technology. The security of the Internet of Things is a critical issue that requires international cooperation and harmonisation of standards to achieve the required effect across diverse markets.

2. It is essential that nations and their people can trust the technology that will underpin their societies now and in the future. Emerging technologies bring a range of opportunities and challenges, including for our approaches to cyber security. We recognise the importance of open, diverse, competitive and trusted critical technology markets, where security-by-design is a fundamental principle. Our nations [redacted] of a joint Statement of Intent, which will align our approaches to enhancing the security of the Internet of Things devices, to provide better protection to users by advocating that devices should be secure by design. The Statement will [redacted] our nations to actively seek out opportunities to enhance trust and raise

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



awareness of best practice associated with IoT devices and reaffirms the need to identify and engage likeminded nations to encourage international alignment on IoT security. We welcome complementary international efforts to improve the security of critical and emerging technologies.

3. In recent years unmanned aircraft systems, often referred to as 'drones', have rapidly evolved in terms of capability, availability, and uptake for commercial and recreational use. Drone technology has the potential to offer significant benefits to economies and quality of life. However, the malicious, unlawful or inadvertent misuse of drones can pose a risk to public safety, be deliberately used to facilitate or commit a wide range of criminal acts, and also present a threat to our national security. We commit to create a stronger approach to drones informed through co-ordinated and in-depth information sharing around threat, vulnerabilities and counter-drone technology. We will also enable the security community to identify what more could be done at the manufacturing stage to mitigate drone risk by design. Work to commence this will begin immediately and the UK will host a event at the Home Office Security and Policing Event in March 2020 to enhance cooperation.

Borders and Asylum

1. Facilitating the legitimate movement of people across our borders is essential to our economic prosperity. We acknowledge the importance of safe and regular immigration and protecting refugees and those seeking asylum and reaffirm the positive benefits that managed immigration, settlement and integration brings to our societies.

2. We recognise the need to modernise border security systems to deal with evolving threats. We therefore commit to pursue expanded data sharing on travellers prior to and at the border to facilitate the secure movement of legitimate goods and in ways that maintain privacy, data security, and are consistent with domestic law.

3. We reiterate the sovereign right of states to strong border management, including the responsibility to deter, prevent, detect and disrupt those who seek to evade or facilitate the evasion of border controls. We also recognise that our ability to deliver timely protection to those genuinely fleeing persecution is hampered by those who abuse or facilitate the abuse of our border and immigration systems, including our asylum systems. We therefore commit to increase our collaboration regarding such activity. We commit to cross-border information sharing on, but not limited to, travelling child sex offenders, in line with domestic legislation. We further reiterate our commitment to work together and with global partners to secure the efficient removal of individuals without lawful status in our countries.

Countering Foreign Interference - Election Security and Strengthening Democracy

1. Building on last year's commitment to establish a mechanism to share approaches to combating foreign interference — being the coercive, deceptive and clandestine activities of foreign governments, actors, and their proxies, to sow discord, manipulate public discourse, bias the development of policy, or disrupt markets for the purpose of undermining our nations and our allies— our countries have shared strategies that protect our electoral institutions and democratic processes from foreign interference and other hostile state activity. We commit to maintaining these efforts, and will continue our collaboration to combat foreign interference in other areas such as the economy and academia.

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



[redacted]

Joint Meeting of FCM and Quintet of Attorneys-General

1. On 30 July, Home Affairs Ministers and Attorneys General met together. We discussed countering child sexual exploitation and abuse, countering violent extremism and terrorism both online and offline, foreign terrorist fighters, and encryption.

Countering Online Child Sexual Exploitation and Abuse

1. We commit to support more effective prevention, disruption and investigative responses to this [redacted]
2. We commit to prioritise the sharing of technology, data and expertise between us to help tackle the global threat of online child sexual abuse, recognising the great benefits that would come from closer cooperation, especially as we explore technologies to respond to new threats such as the live streaming of child sexual abuse.
3. We reaffirm our commitment to the WePROTECT Global Alliance, a partnership of Member States, global technology companies and international and non-governmental organisations working together to end online child sexual exploitation and sexual abuse.

Use of the Internet for Terrorist and Violent Extremist Purposes

1. The internet must not be a safe haven for terrorist and violent extremist content and activity. At the same time, our efforts, including with digital industry, to combat terrorist and violent extremist purposes must be undertaken in a manner consistent with national and international law, including protections for human rights and fundamental freedoms.
2. To this end, we reaffirm our commitment to supporting academic and civil society research on all forms of terrorism and violent extremism, including on the challenges of defining and addressing terrorism and violent extremism, better understanding algorithmic confinement, and developing credible counter and alternative narratives.
3. We commit to continue to work with digital industry to establish protocols for emergency situations, as well as safeguards to protect news reporting.
4. We reaffirm our commitment to engage smaller platforms in addressing their exploitation by violent extremists and terrorists, developing and sharing ways to support their efforts to reduce

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



their exploitation and encouraging industry to work together to share understanding and build capacity to tackle the threat across all platforms.

5. We also commit to support increased information flows between digital industry and the [redacted] including by providing threat-related information to digital industry from the security, intelligence and law enforcement communities to better inform how they moderate content. To build our collective understanding, we also encourage companies to share more data and information about how terrorists exploit their services and their efforts to disrupt this with governments, law enforcement and civil society.
6. We commit to collaborate on progressing the important work that has been undertaken in other likeminded fora, such as the strengthening of the Global Internet Forum to Counter Terrorism and facilitating broad collaboration, drawing on as appropriate the goals of:
    a. The G20 Osaka Leaders' Statement on Preventing the Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism; and
    b. The Christchurch Call to Action.
7. We call on the Countering Violent Extremism Working Group to facilitate information and knowledge exchange on all forms of violent extremism and terrorism.

Online Safety and Encryption

[redacted]

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Foreign Terrorist Fighters

1. Whilst Da'esh has lost the territory of the so-called 'caliphate', as an international community we remain vigilant against terrorism and the continued threat posed by Foreign Terrorist Fighters (FTFs). Within Syria and Iraq, Da'esh has transitioned back to its covert insurgency roots. Some of its members continue to pose a threat both in the region and more widely, whilst others are detained and best efforts must be made to bring them to justice.

2. [redacted] must continue to take the lead in addressing the issue of FTFs effectively, both in our own countries, and providing appropriate support to those countries most affected. We commit to maintain the international focus on addressing both relocating FTFs, and those now in detention. We commit to:

   - Take steps to coordinate, deconflict and prioritise our respective capacity building overseas in third countries, including through effective use of multilateral organisations such as United Nations (UN), and the Global Counter Terrorism Forum (GCTF).

   - Support third countries to fully implement UN Security Council Resolution (UNSCR) 2396, including providing support to build capability to collect, process and analyse Advance Passenger Information (API) and Passenger Name Record (PNR) data, to collect and use biometric data, to develop terrorist watchlists and share watchlist information, and contribute to and use Interpol databases, with full respect for human rights and fundamental freedoms, for the purpose of preventing, detecting and investigating terrorist offenses and related travel.

   - Support the International Civil Aviation Organisation (ICAO) PNR Task Force to establish a global standard for the responsible use and protection of PNR data that can resolve conflicts of law that inhibit the international transfer and processing of PNR data, as well as to support the work of the UN to build Member States' capability to collect, process and analyse API and PNR data.

   - Work together to promote Battlefield Evidence best practice and guidelines to improve global standards for the collection and use of Battlefield Evidence in investigative and judicial processes, including the Guidelines on the collection, use and admissibility of military-collected information presently under development by the UN.

   - Share frameworks and tools between the [redacted] on managing residual risk.

[redacted]

Conclusion

1. We reaffirm today the critical importance of the five country partnership. Bound by our history of cooperation, united by our shared values, and strengthened by our enduring friendship, we pledge the commitments made today as we seek to share opportunities and address security challenges together.

s.15(1) - Int'l
s.16(1)(a)(i)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED
For Official Use Only

BILATERAL MEETING WITH WILLIAM BARR, U.S. ATTORNEY GENERAL

Strategic Objectives

- Highlight the strong relationship and cooperation between Canadian and American law enforcement agencies, and issues of common interest, such as combatting opioids, cybercrime (notably telemarketing and elder fraud) and information sharing [redacted]
- Respond to inquiries about Canada's approach to foreign terrorist fighters and battlefield evidence; as well as encryption.

Key Messages

Law Enforcement Cooperation

- We share common responsibilities regarding domestic law enforcement agencies, and priorities such as opioids and cybercrimes in the field of national security and public safety.
- There are many examples of successful law enforcement cooperation to date, notably between Canadian agencies, the FBI, ATF, and DEA, including:

[redacted]

Opioids

- There is a common challenge of the opioid crisis and rising problem of methamphetamines on both sides of the border.
- Bill C-37, passed in May 2017, provided new measures to better equip law enforcement and health officials to reduce harms linked to drug and substance use.
    - Notably, it provided the authority to border officers to open packages weighing 30 grams or less, and to take action to prevent the uncontrolled import into Canada of devices that can be used to manufacture illicit drugs.

s.13(1)(a)
s.15(1) - Int'l
s.15(1)(e)
s.15(1)(g)
s.16(1)(a)(i)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Prime Minister Trudeau and President Trump agreed in June to work to develop joint actions.

[redacted] the successful trilateral cooperation under the North American Drug Dialogue.

s.21(1)(c)

- China remains the main source of opioids entering Canada [redacted]

- What are your views on the main law enforcement challenges related to opioids and are there lessons learned you would share about U.S. efforts?

Information Sharing [redacted]

- There are robust, collaborative relationships between Canadian security and intelligence communities and their American counterparts.

- Canada is committed to timely information sharing with partners regarding national security threats that impact our countries and shared border – in a manner that protects the rights and privacy of Canadians.

[redacted]

Telemarketing and Elder Fraud

[redacted]

s.15(1) - Int'l
s.15(1)(g)
s.16(1)(a)(i)
s.16(1)(b)
s.21(1)(c)

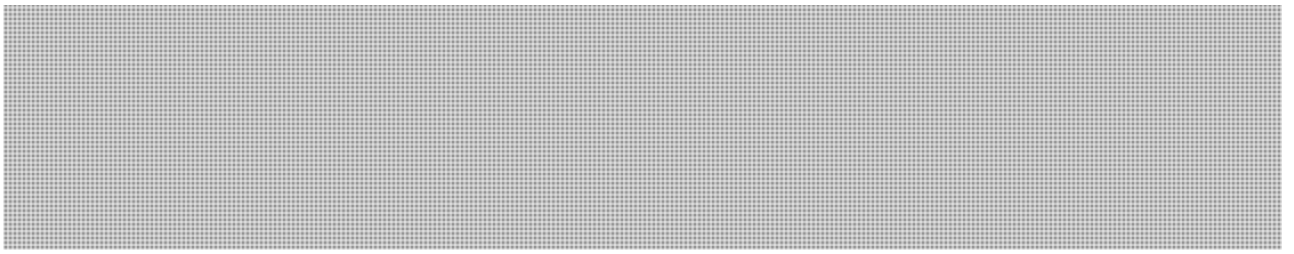
Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- There are partnerships with the provinces and industry that the Government has invested in to combat these types of crimes and support and educate vulnerable populations such as:
  - The RCMP hosted a national mass marketing fraud strategy meeting in May 2018, with local, provincial, and international policing partners, including U.S. Postal Inspection Service and Federal Trade Commission.
  - The RCMP supported the recent U.S. Department of Justice elder fraud initiative through the International Mass Marketing Fraud Working Group, where the RCMP played a key role in tackling the India Call Centre Fraud.
  - The work carried out by the Canadian Anti-Fraud Centre, which serves as a model around the world, including Canada's Fraud Prevention Forum and Fraud Prevention Month, and continuous efforts to support investigations.

Responsive

Foreign Terrorist Fighters and Battlefield Evidence

- Canada takes the threats posed by foreign terrorist fighters seriously and is actively pursuing a whole-of-government approach to monitor and respond to this threat.
  - Criminal prosecution is a top priority and the preferred course of action.



  - Information must be collected, handled, and processed to satisfy the admissibility requirements for legal evidence, and ensure that post-collection chains of custody adhere to the highest evidentiary standards.

Encryption

- Canada is acutely aware of the difficulties for law enforcement agencies as a result of the widespread adoption of encryption, but the public narrative is very much in favor of an increasing the use of encryption.
- The Five Country Ministerial should make clear that we do not seek to undermine the security of communications services or restrict the spread of in-demand encryption technologies, in accordance with past public statements.



s.13(1)(a)
s.15(1) - Int'l
s.16(1)(a)(i)
s.21(1)(a)
s.21(1)(c)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Background

This will be your first meeting with Attorney General (AG) William Barr. It will be an opportunity for you to highlight the strong relationship between law enforcement organisations, and discuss a few common priorities (opioids, [redacted] and combating mass marketing fraud targeted at the elderly).

On June 26, Justice Minister Lametti had his first meeting with the AG and discussed many of the same issues, including [redacted] elder fraud, opioids and battlefield evidence. Given the overlap of topics, Justice Canada's Associate Deputy Minister François Daigle and Assistant Deputy Minister Elisabeth Eid will also be participating in this meeting.

Areas of overlap between the U.S. Department of Justice (DoJ)'s portfolio and that of Public Safety Canada (PS) includes: the FBI and its Terrorism Screening Center (TSC); the DEA; the ATF; United States Marshals Service, and the Bureau of Prisons. There is successful operational cooperation across the PS Portfolio with these agencies to ensure border integrity, cooperate collaborate on law enforcement investigations, and identify threats early.

Existing Law Enforcement Cooperation

[redacted]

Opioids

In early 2017, in order to reduce the supply of opioid and related organized crime activities, the RCMP, CBSA and Canada Post Corporation formed the Organized Crime Joint Operations Centre, which provides tactical support to opioids-related investigations by collecting, analyzing and sharing information and intelligence in relations to opioid importation, production and trafficking. This collaboration has led to investigations and arrests of opioid traffickers in Ontario, Quebec, Manitoba and British Columbia.

Canada-U.S. law enforcement cooperation is key in combatting the opioid crisis. For instance, the RCMP and DEA's continued partnership has resulted in the takedown of five different drug vendors operating on the dark web. In the past four months alone, the DEA has seized multi-kilo shipments of fentanyl, heroin, and cocaine in north eastern states. These seizures point to larger and more sophisticated operations, potentially indicating the growing involvement of Mexican cartels in the trafficking of opioids to North America.

On June 20, the Prime Minister and President committed to develop an action plan to address the opioid crisis, through enhanced law enforcement cooperation, sharing of information and best practices. [redacted] These efforts will include the trilateral work being done with Mexico under the auspices of the North American Drug Policy Dialogue (NADD), such as discussions of ways to improve data collection and sharing on drug

s.13(1)(a)
s.15(1) - Int'l
s.15(1)(a)
s.15(1)(c)
s.15(1)(g)
s.21(1)(a)
s.21(1)(c)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

seizures, smuggling, and illicit financing and money laundering. Canada hosted the NADD in Ottawa last November, and the U.S. is set to host the next meeting in D.C. in December. Through the NADD, the RCMP developed the second Trilateral Opioids Threat Assessment in partnership with the DEA and Mexico's Criminal Investigation Agency on National Drug Policy, which also noted the rise of Mexican cartels in the illicit fentanyl trade.

[redacted]

Telemarketing and Elder Fraud

In Canada, mass marketing fraud is considered a local police matter although most cases are national and international in scope. Jurisdictional issues pose significant challenges to the investigation and prosecution, as most cases can involve evidence in at least three different countries. The RCMP works with local law enforcement partners in Canada and foreign partners through the International Mass-Marketing Fraud Working Group, including the U.S., Belgium, Europol, the Netherlands, Norway, Spain and the UK.

Federally, telemarketing fraud is headed by the Canadian Anti-Fraud Centre (CAFC) which collects information and criminal intelligence on mass marketing fraud, advanced fee fraud, Internet fraud and identification theft complaints. The Centre is jointly managed by the RCMP, the Competition Bureau and the Ontario Provincial Police. The RCMP leads day-to-day operations. The CAFC manages more than 300,000 calls and 60,000 online fraud reports from Canadians and others world-wide annually, generating more than 70,000 complaints each year. CAFC's Senior Support Unit also offers support and advice to senior victims.

The Trump Administration has made the investigation and prosecution of telemarketing and elder fraud a priority. In March, the U.S. announced the largest nationwide sweep of elder fraud cases in history, involving more than 260 defendants from all parts of the world. In June, the AG established a Transnational Elder Fraud Strike Force, which focuses on investigating and prosecuting individuals and entities associated with foreign fraud schemes affecting American seniors. [redacted]

s.13(1)(a)
s.15(1) - Int'l
s.15(1)(a)
s.15(1)(c)
s.15(1)(g)
s.21(1)(a)
s.21(1)(c)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Responsive

Foreign Terrorist Fighters (FTFs) and Battlefield Evidence

[redacted]

In September 2017, the U.S. Department of State (DOS), Department of Defense (DOD) and U.S. DoJ launched a battlefield evidence initiative to assist partner nations in using battlefield evidence effectively in civilian criminal justice proceedings. Based on the key issues and themes highlighted during the the interagency working group discussions, DOS, U.S. DoJ, and DOD collectively developed fourteen non-binding guiding principles. [redacted] Other like-minded countries like Denmark and the Netherlands have also had some success. [redacted]

Encryption

The U.S. is renewing its push to have technology companies help law enforcement break encryption. On July 23, at a cybersecurity conference hosted by the FBI and Fordham University in New York, the AG noted that companies may soon be required to act to respond to a "dangerous and unacceptable" status quo [redacted] The FBI Director will echo concerns about "the damage being inflicted" by the use of encryption, when he speaks at the conference on Thursday. Should the AG raise this issue, you may wish to note Canada's approach.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BIOGRAPHY

William Barr - Attorney General, United States



William Barr was confirmed by the U.S. Senate as the 85th United States Attorney General in the Trump administration on February 14, 2019.

From 1973 to 1977, he served in the Central Intelligence Agency before receiving his J.D. with highest honors from George Washington University Law School in 1977.

In 1978, Mr. Barr served as a law clerk with the U.S. Court of Appeals for the District of Columbia Circuit, before working in the private sector. He served in the White House under President Ronald Reagan from 1982 to 1983 on the domestic policy staff, before returning to private practice.

Mr. Barr also served as Attorney General under George H.W. Bush from November 1991 to January 1993. He went on to serve as Executive Vice President and General Counsel for GTE Corporation from 1994 to 2000, and as Executive Vice President and General Counsel for Verizon from 2000 to 2008, when he retired.

Prior to being nominated for the Attorney General by President Trump, Mr. Barr worked for Kirkland & Ellis LLP, since 2017.

Attorney General

The United States Attorney General is the chief lawyer of the Federal Government of the United States and the head of the U.S. Department of Justice (DOJ). The Attorney General's responsibilities include:

- Representing the U.S. in legal matters;
- Providing advice and opinions on legal matters to the President, Cabinet and heads of executive departments and agencies;
- Making recommendations to the president on federal judicial appointments;
- Supervising and directing the Department of Justice; and
- Overseeing law enforcement agencies under DOJ purview, including the FBI, Drug Enforcement Administration, and National Institute of Corrections.

s.15(1) - Int'l
s.15(1) - Subv
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED
FOR OFFICIAL USE

TRILATERAL MEETING WITH MINISTER HUSSEN AND DAVID PEKOSKE U.S. ACTING DEPUTY SECRETARY OF HOMELAND SECURITY

Strategic Objectives

- Provide updates on Canadian terrorist listings, and approaches to 5G.
- Respond to:
  - [redacted]
  - [redacted]
  - any information shared on timely updating of U.S. Customs and Border Protection records to reflect cannabis pardons.
- [redacted]

Key Messages

Terrorist Listings

- Highlight the recent *Criminal Code* listings, including:
  - two right-wing extremist entities with a presence in Canada: Blood & Honour and Combat 18; and,
  - three Iran-backed proxy terrorist groups already designated by the U.S.: Harakat al-Sabireen, Fatemiyoun Division, and Al-Ashtar Brigades.
- Raise the prospect of listing a specific entity in concert with the U.S.

5G

- Highlight that Canada is carefully examining the security challenges and potential threats involved in 5G technology, while recognizing the importance that this technology holds in the continued development of a dynamic digital economy.
- Note that, since 2013, the Communications Security Establishment's Security Review Program has been in place to help mitigate risks in Canadian 3G and 4G/LTE networks by testing and evaluating designated equipment and services, [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Responsive

[redacted]

Extremist Travelers

- Stress that Canada takes the threats posed by foreign terrorist fighters seriously and is actively pursuing a whole-of-government approach to monitor and respond. Criminal prosecution is a top priority and the preferred course of action.
- Reiterate that, given the security situation on the ground, the Government of Canada's ability to provide consular assistance in any part of Syria is limited.
- [redacted]

Cannabis Legalization and Data Retention

- [redacted]
- Emphasize the importance of criminal records kept in the U.S. reflecting the accurate legal status of Canadians so that U.S. decisions are based on complete and accurate information.
- [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Background

Given Acting Deputy Secretary Pekoske's schedule, the U.S. has requested a 30 minute trilateral meeting with you and Minister Hussen. This will be your first meeting with the Acting Deputy Secretary, but it will follow upon your last meeting with Acting Secretary McAleenan on June 10 in D.C. where you discussed various issues including: the dangerous use of social media, returning foreign fighters, 5G Exit/Entry and Preclearance. There is limited time allotted for the trilateral meeting,

As such, topics recommended for you to proactively raise are targeted.

Terrorist Listings

On June 26, Canada published an update to the *Criminal Code* list of terrorist entities that included, for the first time, two right wing extremism groups with a presence in Canada: Blood & Honour, and Combat 18. Three Iranian-backed proxy terrorist groups (Harakat al-Sabireen, Fatemiyoun Division, and Al-Ashtar Brigades), already designated by the U.S. were also added.

5G

The U.S. has continued to implement legal mechanisms related to 5G, while strongly encouraging its allies to carefully weigh the security considerations of 5G technology. On May 15, 2019, President Trump signed an Executive Order which outlined a variety of measures on 5G and other Information and Communications Technologies (ICT) intended to protect U.S. national security and economic interests. The Order prohibits U.S. firms from commercial ICT transactions with 'adversaries' who pose a specific threat. Immediately following, the Department of Commerce announced new export control measures targeting Huawei and 68 non-U.S. Huawei affiliates (including Huawei Canada). With their addition to the Entity List, U.S. vendors wishing to sell or transfer technology to Huawei and its affiliates are required to apply for a license before doing so. The Department of Commerce has issued a 90 day temporary general license to prevent the interruption of existing contracts and operational activities.

At the G20 in June, President Trump indicated that U.S. firms may be able to continue selling products to Huawei despite being on the Entity List. The U.S. has since clarified that while Huawei will remain on the List, licenses will be issued for the sale of goods where there is no threat to national security.

At your June meeting with Acting Secretary McAleenan, you agreed to share an update on 5G when you next met

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Responsive

[redacted]

Extremist Travelers

Both countries are looking to increase the ability to prosecute and convict returning foreign fighters. [redacted]

Cannabis Legalization and Data Retention

While presenting Bill C-93 at the House of Commons Standing Committee on Public Safety and National Security, you committed to reaching out to the U.S. about their data retention policies. This is to avoid cases of conflicting information where U.S. Customs and Border Protection (CBP) retains copies of historical data or records that does not reflect the issuance of a pardon for cannabis possession. [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



David P. Pekoske, Acting Deputy Secretary for Homeland Security

On April 10, 2019, David Pekoske was designated by Acting Secretary of Homeland Security Kevin K. McAleenan to serve as the Senior Official Performing the Duties of the Deputy Secretary. He was confirmed by the U.S. Senate as the seventh Administrator of the Transportation Security Administration in August 2017.

TSA's workforce of approximately 60,000 employees, including the Federal Air Marshal Service, ensures security of transportation systems across the United States, and operates a robust aviation security system at over 440 domestic airports. Under Pekoske's leadership, TSA has raised the security baseline for both aviation and surface transportation through close partnerships and alliances, and a robust homeland security network.

Before joining TSA, Pekoske was an executive in the government services industry where he led teams that provided counterterrorism, security and intelligence support services to government agencies. Most notably, Pekoske served as the 26th Vice Commandant of the U.S. Coast Guard culminating a Coast Guard career that included extensive operational and command experience. As the Vice Commandant, Pekoske was second in command, also serving as Chief Operating Officer and Component Acquisition Executive of the U.S. Coast Guard. He is a recognized expert in crisis management, strategic planning, innovation and port and maritime security.

Pekoske holds a Master of Public Administration degree from Columbia University and a Master of Business Administration degree from the Massachusetts Institute of Technology. He earned his Bachelor of Science degree in ocean engineering from the U.S. Coast Guard Academy. His awards include the Homeland Security Distinguished Service Medal, Coast Guard Distinguished Service Medal, the Meritorious Service Medal, Coast Guard Commendation and Achievement Medals.

s.15(1) - Int'l
s.21(1)(c)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

MEETING WITH PRITI PATEL
HOME SECRETARY OF THE UNITED KINGDOM

Strategic Objectives

[redacted]

- Register the Canadian approach to the issue of encryption with the Home Secretary.
- Strengthen Canada's cooperation with the UK against hostile state activities.

[redacted]

Key Messages

Preventing Violent Extremism, including Right Wing Extremism

- Advise the Home Secretary about Canada's addition of Blood & Honour and Combat 18 to the *Criminal Code* list of terrorist entities.
- Highlight Canada and the UK's continued efforts to prevent and counter violent extremism, including online.

Broader Online Harms (including Terrorist Use of the Internet and Child Sexual Exploitation)

Relationship with technology companies

[redacted]

- Reiterate that technology companies should continue to be called upon to improve transparency and engagement with governments, including law enforcement.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Seek the Home Secretary's view on reforming the Global Internet Forum to Counter Terrorism.

Child Sexual Exploitation and Abuse

- Underscore that Canada's Project Arachnid is being supported by the UK Home Office and allows for unprecedented collaboration between Canada and the UK in identifying child sexual exploitation images for removal from the Internet.

- Emphasize that the Canadian Centre for Child Protection is a non-governmental organization and a key partner under Canada's strategy to combatting child sexual exploitation online,

Encryption

- Stress that Canada is acutely aware of the difficulties for law enforcement agencies as a result of the widespread adoption of encryption, but that the public narrative on this issue is very much in favor of an increasing the use of encryption.

- Ask how the UK is progressing in terms of strengthening the public narrative on this sensitive issue. Seek insight from the UK active engagement in the public debate on encryption and with stakeholders from the industry.

- Emphasize the importance for the Five Country Ministerial to make clear that we do not seek to undermine the security of communications services or restrict the spread of in-demand encryption technologies, in accordance with past public statements.

- Highlight that Canada supports deepening the partnership between investigative agencies and service providers and building stronger relationships with industry, in the belief that progress can be made if governments are kept informed when decisions regarding new products and services are made.

Hostile State Activities

- Note that Canada is implementing new measures aimed at safeguarding our democratic process against foreign interference in anticipation of the fall

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

general election, and seek to learn more about the UK's approach and the best practices they have adopted.

Foreign Terrorist Fighters

- Stress that Canada is pursuing a whole-of-government approach to monitor and respond to this threat. Criminal prosecution is a top priority and the preferred course of action.

- Emphasize the importance of the Five Country Ministerial presenting a unified vision for managing and mitigating the threat posed by foreign terrorist fighters to ensure the safety of each respective country's citizens, while upholding democratic values and human rights obligations.

- [redacted]

Terrorist Listing

- Share information on Canada's intent to add an additional entity to its *Criminal Code* list of terrorist entities, potentially in concert with the UK.

Background

This is your first meeting with Secretary Patel. You had a bilateral meeting with former Home Secretary Javid in April 2019 at the G7 Interior Ministers' meeting in Paris. You discussed violent right-wing extremist (RWE) groups, including the inclusion in 2016 of a racist neo-Nazi group on the UK's list of proscribed terrorist organizations. You also exchanged perspectives on the potential regulation of digital industry, with Secretary Javid outlining the UK's White Paper on Online Harms. [redacted]

You will be meeting Secretary Patel together with Minister Hussen, who plans to ask about irregular migration, the Global refugee sponsorship initiative and settlement and integration in the UK.

Violent Right-Wing Extremism (RWE) and Violent Extremist and Terrorist Use of the Internet (VETUI)

On June 26, Canada published an update to the *Criminal Code* list of terrorist entities that included, for the first time, two RWE groups with a presence in Canada: Blood & Honour (B&H), and Combat 18 (C18). Both groups were founded in the UK.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Canada and the UK both recently participated in the Christchurch Call to Action Summit on May 15, 2019, hosted by New Zealand Prime Minister Ardern and French President Macron.

Canada and the UK also recently joined the G20 Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism. It encourages digital industry to bolster their efforts to prevent and counter VETUI, as well as preserve content for evidentiary purposes. It also encourages reform and expansion of the Global Internet Forum to Counter Terrorism (GIFCT, led by Facebook, Google, Microsoft and Twitter).

Broader Online Harms

The UK is taking a broad online harms approach to combatting VETUI, child sexual exploitation and abuse (CSEA) and foreign interference and disinformation. The Cabinet Office's National Security Secretariat provides an internal coordination function for all content policy. The Home Office is still responsible for online counterterrorism.

In April 2019, the UK government released an Online Harms White Paper as a precursor to bringing forward online safety legislation to address terrorist use of the internet, CSEA online, disinformation, gang culture and violence, and bullying and psychological abuse. The White Paper recommends reinforcing the role of technology in the development of solutions, building a global coalition of countries, and renewing public confidence in technology companies. It also proposes the development of a new regulatory framework for digital industry based on a "duty of care", as well as the development of a new independent regulator to enforce this framework. The Government Response to the White Paper is expected to be tabled in fall 2019.

The Canada Centre is attending the upcoming annual GIFCT Summit in California at the end of July and expects GIFCT companies to announce new initiatives to better address the threat of VETUI.

The GIFCT is actively working on ways to become more effective in its activities and partnerships with government and civil society, but is in need of reform. In a Five Eyes context, our contribution to this process may be best led at the working level, such as through the Digital Industry Senior Officials Group (DIESOG).

Child Sexual Exploitation and Abuse (CSEA)

For the most serious online offending such as terrorism and CSEA, the UK White Paper proposes that companies go much further than for other harms, and demonstrate the steps taken to combat the dissemination of associated content and illegal behaviours.

In Canada, the RCMP's National Child Exploitation Coordination Centre (NCECC) is the central point of contact for investigations related to online CSEA. In 2016, the Canadian Centre for Child Protection (C3P) launched Project Arachnid, a technological tool which identifies child sexual

exploitation images for removal from the Internet, which is also being supported by the UK Home Office and allows for unprecedented collaboration between Canada and the UK in the field.

C3P is very supportive of the UK approach to CSEA, including its work to engage with the digital industry to put in place a set of voluntary guiding principles and best practices to guide their role in addressing CSEA.

[redacted]

Data and technology sharing is a crucial component of law enforcement's ability to address online child sexual exploitation and abuse internationally. Canada is supportive of enhanced information sharing related to investigational data, technological challenges, requirements and solutions; however there is a need to distinguish between technology and criminal-related personal information sharing. Canadian privacy protection legislation and our constitutional framework require maintaining the case-by-case approach for personal information sharing.

In Canada, the Sex Offender Information Registration Act (SOIRA), which was implemented in 2004, and the National Sex Offender Registry (NSOR) established thereunder, is the federal database of convicted sex offenders (child and otherwise) in Canada. The NSOR is administered by the RCMP and accessible to all accredited Canadian police agencies for specific preventive or investigative purposes through provincial/territorial registration centre. The NSOR is an offence-based model and inclusion is automatic upon conviction for a range of sex offences; it is not determined by the offender's level of risk.

Canadian law enforcement officials are authorized to disclose to foreign police services information collected under SOIRA or under the NSOR, on a case by case basis as long as the threshold is satisfied specifying that sharing information is necessary to assist a police service outside Canada with the prevention or investigation of a crime of a sexual nature. Prohibitions on systematic disclosure of this information ensure consideration of the registered sex offender's privacy interests and fundamental rights under the Canadian Charter of Rights and Freedoms.

Encryption

2018 Statement of Principles on Access to Evidence and Encryption

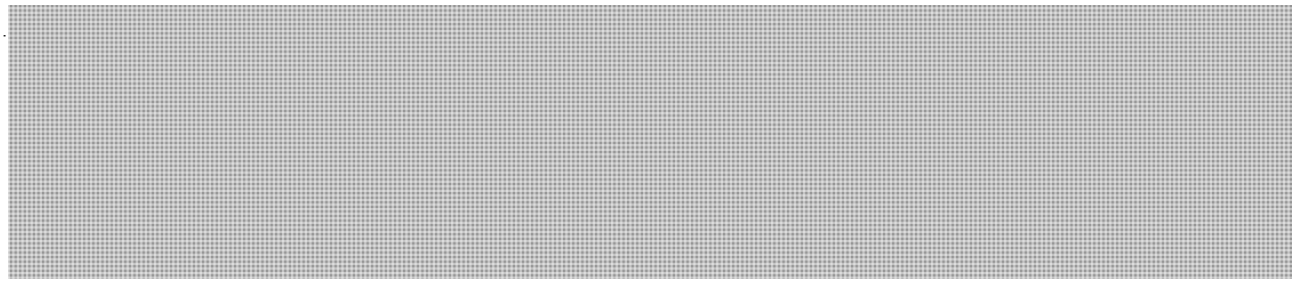
As part of last year Five Country Ministerial meeting, the Five Eyes released a Statement of Principles on Access to Evidence and Encryption. The statement stressed the importance of encryption to cybersecurity, as well as the challenges it creates for law enforcement and national security agencies. The need to cooperate with providers of information and communications technology and services was emphasised. Finally, the statement underscored the importance of the rule of law and due process, as well as the freedom of choice for Five Eyes countries to address encryption as they see fit.

The Statement of Principles garnered some media attention, and some criticism. The particular focus of criticism and comments was on what was characterized as a threat made by the five

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Governments; which was that if service providers did not voluntarily assist in providing unencrypted data, that Governments retain the right to proposed "technological, enforcement, legislative or other measures to achieve lawful access solutions".

Existing solutions

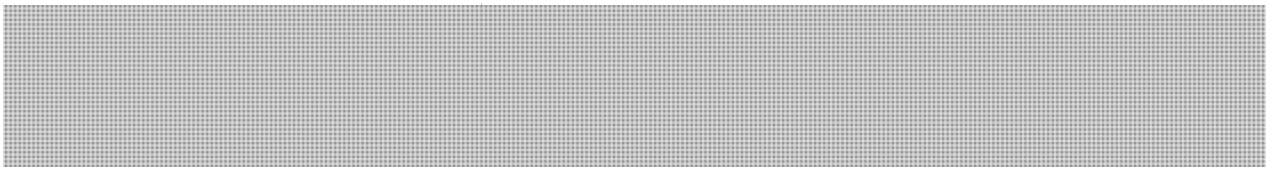


Public debate and stakeholders' engagement

While CSPs are receptive to engaging on encryption, they have strongly opposed attempts by governments to mandate access to encrypted data in ways that would undermine the security of their products or jeopardize the trust of their users. When faced with coercive government actions, CSPs have not hesitated to challenge them in court. For example, the associations representing major US CSPs filed amicus briefs in support of Apple during 2016 litigation over access to a dead terrorist's encrypted iPhone. Given the importance of protection of cybersecurity, these concerns would need to be fully addressed by any government policy that attempts to assist law enforcement with the challenge of encryption, both from a substantive perspective, and from a communications perspective.

Another challenge in this respect is that even if the requirements imposed do not in fact inherently weaken the protection provided by encryption, concerns regarding this possibility will likely continue to strongly influence the views of the public and stakeholders, and raise significant privacy concerns.

Hostile State Activity (HSA)



The UK has launched a parliamentary review of the impact of disinformation during the Brexit Campaign. Following its investigation on the roles played by Facebook and Cambridge Analytica, the Parliamentary Committee on Digital, Cultural, Media and Support (DCMS) published an interim report on July 29, 2018. The report outlined the incident, the threats, and provided recommendations to the Government.

s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Like Canada, the UK is a member of the European Union Centre of Excellence on Hybrid Warfare (Hybrid CoE). The UK is a member of the G7 Rapid Response Mechanism (RRM), led by Canada, established at the G7 Summit in June 2018.

Foreign Terrorist Fighters (FTFs)/Returns

A successful initiative within CONTEST, the UK counter-terrorism strategy, is the Channel program, which involves local police, health, and community agencies who come together to assess cases and design tailored interventions to guide individuals away from violent extremism.

The UK's *Terrorism Act* provides stop and search powers to assist police and border forces in the prevention, disruption, and detection of terrorism. Among measures available, Terrorism Prevention and Investigation Measures, which are similar to Canada's Peace Bonds, can be issued by the Home Secretary.

The Home Secretary may deprive individuals of their citizenship through executive power. Between 2006 and March 2019, the Home Secretary denaturalized 373 Britons, 53 of whom had alleged links to terrorism. The UK Home Secretary takes the decision to denaturalize British citizens on a case-by-case basis, with the direction of the Government of the UK legal counsel. Under international law, the UK can only revoke citizenship of a dual national. The UK is not permitted to revoke citizenship to make an individual stateless.

[redacted]

Recently, the US and Kurdish authorities have requested source countries to repatriate their nationals. Canada has thus far not repatriated any of its nationals, including children. Under section 6(1) of the *Charter of Rights and Freedom*, Canadian citizens have the right to enter Canada; however, in most cases, Canada has no positive obligation to provide repatriation assistance. Canada has no diplomatic presence in Syria and, as such, its ability to provide consular assistance there is extremely limited.

The repatriation of children presents a number of complex challenges. Notwithstanding, concern about the welfare of the children being held in Al Hol has been growing. Pressure from local officials, the UN, non-governmental organizations (NGOs) and activists to repatriate these children based on moral and humanitarian grounds is intensifying. Media attention on this issue has increased significantly since April, when Germany reportedly repatriated several children. Three children have been repatriated to the UK. However, the UK's policy is not to repatriate.

Terrorist Listing

Canada is considering adding additional groups to its *Criminal Code* list of terrorist entities. As part of this process, you may wish to raise the prospect of listing an entity in concert with the UK.

Consulted: CSCCB, NCSB, NSOD, and PACB/Canada Centre.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BIOGRAPHY

Priti Patel – Secretary of State for the Home Department, United Kingdom



Priti Patel was appointed Home Secretary on July 24, 2019, following the election Boris Johnson as the new UK Prime Minister.

Secretary Patel has served as a Member of Parliament for Witham in Essex since 2010. She previously served as International Development Secretary from 2016 to 2017.

Prior to her election as MP, Secretary Patel studied Economics at Keele University. She completed studies in British Government and Politics at the University of Essex.

After graduation, Secretary Patel worked as head of the press office for the Referendum Party from 1995 to 1997. She joined the Conservative party in 1997 and worked in the party's press office until 2000. She was employed at Weber Shandwick, a PR consulting firm, from 2000 until 2003 before moving on to work in corporate relations for the British multinational alcoholic beverages company Diageo. In 2007, she became the Director of Corporate and Public Affairs, before eventually moving on to begin her career as an MP in 2010.

Home Office

The Home Office is the lead government department for immigration and passports, drugs policy, crime, fire, counter-terrorism, and police. The Home Office is supported by the UK's Border Force, Her Majesty's Passport Office, Immigration Enforcement, and UK Visas and Immigration.

The Secretary of State for the Home Department has overall responsibility for the Home Office and supervises the work of its junior Ministers. This includes:

- Security and terrorism;
- Securing the UK border;
- Crime reduction and prevention, including cyber-crime and serious and organized crime;
- Issuing passports and visas, controlling immigration;
- Fire prevention and rescue;
- Legislative programming; and
- Expenditure issues.

s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED
FOR OFFICAL USE ONLY

MEETING WITH ANDREW LITTLE
MINISTER FOR JUSTICE, COURTS AND TREATY OF WAITANGI NEGOTIATIONS OF NEW ZEALAND

Strategic Objectives

- Assure New Zealand of Canada's continued commitment to the Christchurch Call to Action and highlight Canada's listing of two violent right-wing extremist entities.
- Seek information on New Zealand's new Cyber Security Strategy 2019 and New Zealand's firearms ban and buy-back program.
- [redacted]

Key Messages

Preventing Violent Extremist and Terrorist Use of the Internet

- Thank Minister Little for co-leading the Quintet discussion on violent extremism online and offline, and for New Zealand's continued leadership, including the *Christchurch Call to Action.*
- Highlight Canada's effort to combat violent right-wing extremism including the recent listing of two entities with a presence in Canada: Blood & Honour and Combat 18.
- Highlight Canada's recent $1 million commitment to the UN initiative Tech Against Terrorism to help them support smaller companies to better detect and remove terrorist content.
- Note Canada's intent to host the Youth Summit on countering violent extremism online.
- Highlight that senior officials from NZ have been engaging with the Canada Centre for Community Engagement and Prevention of Violence to learn about Canada's experience with Moonshot CVE, including the "redirect method".

s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Cyber Security

- Ask the Minister about New Zealand's new Cyber Security Strategy 2019 noting that Canada will follow its National Cyber Security Strategy with a new National Cyber Security Action Plan.

- Ask the Minister how New Zealand is balancing the security challenges and potential threats involved in 5G technology against the importance of this technology in the development of a digital economy.

Cannabis Legalization

- Reiterate Canada's readiness to collaborate with New Zealand ahead of its binding referendum in 2020 on legislation for cannabis legalization and regulation for non-medical purposes.

Firearms Ban

- Highlight Canada's shared commitment with New Zealand to reduce gun violence, and note that Canada has been examining a ban and compensation program for certain assault-style firearms.

- Ask what successes or challenges have been encountered that Canada could learn from if it does decide to pursue a ban and buy-back program.

Terrorist Listings

- Share information on Canada's intent to add an additional entity to its *Criminal Code* list of terrorist entities.

Indigenous Policing

- If time permits, ask about the Minister's experience regarding engaging Indigenous communities in culturally responsive policing.

- Seek information on the collaborative work of the Māori and New Zealand national police, and ask that officials share information relating to governance, recruitment, and other initiatives.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Background

You met with Minister Little as he attended last year's FCM in Australia, and you called him to offer your condolences in the aftermath of the Christchurch attack on March 15, 2019. Minister Little is your closest equivalent in New Zealand. He is the minister responsible for the Government Communications Security Bureau and the New Zealand Security Intelligence Service. He is also Minister responsible for Justice, Courts, and Treaty of Waitangi Negotiations. Consequently, a large part of his role relates to Indigenous self-governance.

Preventing Violent Extremist and Terrorist Use of the Internet (VETUI)

New Zealand initiated the Christchurch Call to Action after the horrific terrorist attack in Christchurch on March 15, 2019.

While New Zealand is relatively new to the VETUI space, their government has quickly taken an effective leadership role on the international stage in response to the terrorist attack in Christchurch. At the working level, Canada has provided support on a number of issues, especially in research and program design where Canada has significant experience and lessons learned to share. Officials from the two countries have met bilaterally at the working level

[redacted]

New Zealand also led discussions on GIFCT reform and crisis protocols at the recent GIFCT annual summit, held at Facebook's headquarters in California, where Canadian officials both participated and provided support in preparation. Separately, Canada continues to provide lessons-learned and advice to New Zealand on VETUI, including in response to New Zealand's interest in learning more about the work of Moonshot CVE and their Canada ReDirect project, given considerations of potentially investing in similar initiatives.

The collaboration between New Zealand and Canada is already significant, and there is potential to go further given how similar are the approaches to VETUI in the two countries. As the tech sector continues to expand its efforts to address VETUI, close collaboration between Canada and New Zealand could help advance asks of the companies.

Cyber Security

New Zealand's New Cyber Security Strategy 2019

Released on July 2, New Zealand's new *Cyber Security Strategy* emphasizes four key values: the importance of partnerships; the centrality of human rights; the need to enhance economic growth; and the protection of national security. The *Strategy* reiterates New Zealand's dedication to acting as a champion of a free, open, secure internet both at home and abroad. Initiatives include seeking Cabinet approval to accede to the Budapest Convention on Cybercrime, making the law fit-for-purpose to better enable agencies to manage and respond to

s.15(1) - Def

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

cybercrime, and raising the country's ability to respond to objectionable material and terrorist activity online.

National Cyber Security Action Plan

Canada's upcoming National Cyber Security Action Plan will serve as a blueprint for the implementation of the National Cyber Security Strategy (released June 2018). The Action Plan will outline initiatives and milestones supporting each of the Strategy's three goals (secure and resilient systems; an innovative and adaptive cyber ecosystem; and effective leadership, governance, and collaboration).

Fifth Generation (5G)

New Zealand has the ability to restrict the use of equipment and services in 5G telecommunications networks through a case-by-case review of the national security risks of telecommunications service providers' (TSPs) proposed deployments. The case-by-case review process is enabled by the *Telecommunications Interception Capability and Security Act 2013* which requires TSPs to notify the Government Communications Security Bureau of proposed decisions, courses of action, or network changes for security review purposes.

You may wish to note to the Minister that since 2013 the Communications Security Establishment (CSE)'s Security Review Program has been in place to help mitigate risks in Canadian 3G and 4G/LTE networks by testing and evaluating designated equipment and services, and by excluding designated equipment from sensitive areas of Canadian networks.

Cannabis Legalization

While possession of any amount of cannabis is currently illegal in New Zealand, the country's approach has actively shifted away from prosecuting people for use and possession of cannabis over the last few years.

On May 7, 2019, the government confirmed that draft legislation to legalize cannabis for non-medical purposes would be subject to a binding referendum, to be held simultaneously with the September 2020 general elections. The draft legislation would:

- Set a minimum age of 20 to use and purchase recreational cannabis;
- Regulate different forms of cannabis, including cannabis-derived products such as edible cannabis and extracts;
- Limit cannabis consumption to private homes and licensed premises;
- Establish a licensed commercial cultivation and production supply chain; and,
- Provide limited home-growing options.

On May 1, 2019, Minister Blair met with five New Zealand MPs in Ottawa to discuss Canada's approach to the legalization and strict regulation of cannabis.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Firearms Ban

Following the Christchurch attack on March 15, 2019, Prime Minister Ardern announced a ban on military-style semi-automatic weapons, assault rifles and high-capacity magazines and parts, as well as an amnesty and buy-back program. The Bill received Royal Assent in April 2019.

In Budget 2019, the New Zealand Government announced NZ $168 million (CAD $146 million) in new funding for the buy-back program, and that it would seek additional funding if necessary. The ultimate cost is unknown due to the lack of a registry of firearms.

The collection of firearms will be led by the New Zealand Police, with the New Zealand Defence Force providing facilities for secure and safe storage. The New Zealand Transport Agency will assist with transporting firearms from Police to Defence Force bases. Destruction will take place at shredders and smelters, supervised by New Zealand Police.

To date, only about 700 firearms have been surrendered by owners. The lack of uptake may be because owners were waiting for details of the buy-back plan to be published. The buy-back values were published on June 20, 2019; those surrendering new or almost new firearms will be compensated with 95% of their original value, while those with older firearms will be given less. Some firearm owners have expressed dissatisfaction with the amounts being offered as compensation.

Terrorist Listings

Canada is considering adding additional groups to its Criminal Code list of terrorist entities. As part of this process, you may wish to raise the prospect of listing an entity, potentially in concert with New Zealand.

Indigenous Policing

The delivery of culturally-responsive police services is a priority in both countries. New Zealand is currently administering many Indigenous policing initiatives under the framework of the Waitangi Treaty.

The Treaty of Waitangi is New Zealand's founding document which ensures a relationship of partnership, participation, and protection between the government and the indigenous peoples of New Zealand, the Māori. The treaty also ensures that the Māori have authority over their own affairs and are involved in any policies pertaining to them. In the context of policing, the Treaty commits to improving police capabilities to address Māori issues, as well as ensuring engagement with the indigenous group for any decision making that affects the Māori.

The recently released *Final Report of the National Inquiry into Missing and Murdered Indigenous Women and Girls* contained recommendations related to Indigenous policing,

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

notably a Call for Justice which called upon all levels of government to work together to move Indigenous policing from an exercise in mere delegation to one of self-governance and self-determination by replacing the FNPP with a new legislative and funding framework.

In Canada, through the First Nations Policing Program (FNPP), the Government of Canada provides support for the provision of professional, dedicated and culturally-responsive policing services to First Nation and Inuit communities across Canada. The financial contribution for agreements under the FNPP is cost-shared between Canada and the provinces and territories.

Consulted: PACB/Canada Centre, NCSB and CSCCB.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BIOGRAPHY

Andrew Little – Minister for Justice, Courts, and Treaty of Waitangi Negotiations, New Zealand



Minister Little was appointed Minister for Justice, Courts, and Treaty of Waitangi Negotiations with the formation of the Labour-led coalition government on 26 October 2017.

Minister Little studied law and philosophy at Victoria University of Wellington, where he also headed the Victoria University Students' Association and New Zealand Union of Students Associations.

After graduation Minister Little became a lawyer with the Engineers Union, where he worked with the Accident Compensation Corporation on employment law, eventually becoming the union's general counsel. In 2000, he was appointed national secretary of New Zealand's largest trade union, the Engineering, Printing, and Manufacturing Union (EPMU) and led the union for a decade.

Minister Little entered Parliament in 2011 and stood as Leader of the Opposition from 2014 until his resignation in 2017, when he was appointed as a Cabinet Minister.

Portfolio:

Minister Little's portfolio includes:

- Government Communications Security Bureau;
- New Zealand Security Intelligence Service;
- Justice policy;
- Law courts;
- Pike River Re-entry department; and
- Treaty of Waitangi negotiations

s.15(1) - Def
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

UNCLASSIFIED
FOR OFFICAL USE

MEETING WITH PETER DUTTON
MINISTER FOR HOME AFFAIRS, AUSTRALIA

Strategic Objectives

- Highlight cooperation between Canada and Australia on preventing violent extremist and terrorist use of the internet (VETUI), as well as Canada's recent right-wing extremist listings.
- [redacted]
- Discuss Australia's strategy of preventing foreign interference in its recent election.
- Highlight Canada's 2019 budget commitment to help protect the cyber security of critical infrastructure with a new critical cyber systems framework.
- Discuss Canada's expanded strategy on combatting the exploitation of children and the focus on engagement with digital industry.

Key Messages

Preventing Violent Extremist and Terrorist Use of the Internet

- Acknowledge Australia's leadership at the recent G20 in Osaka in getting the statement on "Preventing Exploitation of the Internet For Terrorism and Violent Extremism Conducive to Terrorism" adopted by all G20 leaders.
- Ask about Australia's *Sharing of Abhorrent Violent Material Bill*, which calls for digital industry in Australia to proactively and expeditiously remove illicit content from their platforms, and imposes harsh penalties on digital industry executives who fail to do so.
- Highlight Canada's effort to combat violent right-wing extremism including the recent listing of two entities with a presence in Canada: Blood & Honour and Combat 18.
- Note Canada's new initiatives including committing funds to Tech Against Terrorism to help them support smaller companies better detect and remove content from their platforms, and the plan to host a Youth Summit on countering violent extremism online in collaboration with the GIFCT.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Foreign Terrorist Fighters

- Ask about Australia's recent experience repatriating orphans of foreign terrorist fighters.

Hostile State Activity / Foreign Interference

- Ask about Australia's experience in preventing foreign interference in its recent 2019 election. Highlight Canada's proactive approach to safeguard the 2019 General Election from threats such as hostile state activity.

- Discuss Canada's efforts to counter hostile state activity more broadly, including in the areas of economic security, academic institutions and other sensitive sectors.

Cyber Security

- Ask about Australia's approach to protecting the cyber security of non-government cyber infrastructure.

- Highlight Canada's new National Cyber Security Action Plan, which lays out the specific initiatives planned over the coming five years to bring the National Cyber Security Strategy to life.

Terrorist Listing

- Share information on Canada's intent to add an additional entity to its *Criminal Code* list of terrorist entities, potentially in concert with Australia.

Background

You met with Peter Dutton at last year's FCM in Australia and signed a Memorandum of Understanding (MOU) on emergency management cooperation.

Preventing Violent Extremism and Terrorist Use of the Internet (VETUI)

Australia has taken a strong approach to regulation. In the wake of the Christchurch attack, Australia passed the *Sharing of Abhorrent Violent Material* bill, which creates new criminal offences for internet service providers, content service providers, and hosting services that fail to notify the Australian police about, or fail to expeditiously remove, videos depicting abhorrent violent content. Online platforms that fail to remove such content quickly could face fines of up to 10% of their Australian annual profit, and employees could be sentenced to up to three years in prison. Companies must also inform police when illegal material is found.

s.13(1)(a)
s.15(1) - Int'l
s.16(1)(c)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

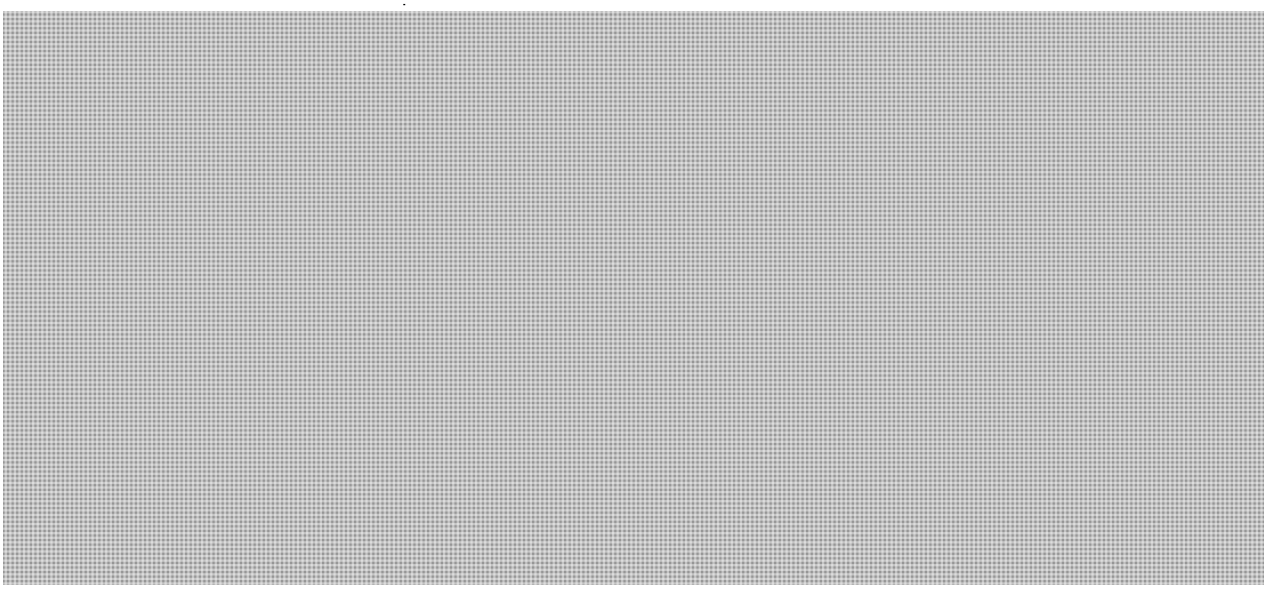
Canada and Australia recently participated in the Christchurch Call to Action Summit on May 15, 2019 in Paris.

Canada recently joined the Australia-led G20 Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism. It encourages digital industry to bolster their efforts to prevent and counter VETUI, as well as preserve content for evidentiary purposes. It also encourages reform and expansion of the Global Internet Forum to Counter Terrorism (GIFCT).

In addition to close collaboration with the law enforcement, security and intelligence communities, as well as the Digital Industry Engagement Senior Officials Group (DIESOG), Canada and Australia are working closely together on research and development related to countering violent extremism (CVE). This includes through the FCM Five Country Research & Development Network (the '5RD'), where an area of focus is collaborative investment on systematic evidence reviews on what works for CVE.

Additionally, Canada and Australia are collaborating on R&D related to CVE through the Community Resilience Fund (CRF). The CRF is supporting a new project led by Ryerson University to replicate applied research originally conducted in Australia, to understand the experiences of those who have shared, or who would consider sharing, concerns with authorities about "intimate" others related to suspected involvement in violent extremism activity. The CRF is also funding research led by University College London in partnership with Canadian researchers, on testing the reliability, validity and equity of terrorism risk assessment tools. Australia is funding additional research of Australian National University that builds on this.

Further opportunities exist for collaboration between Australia and Canada in areas such as measures to assess progress in management of high-risk cases, and to learn from experiences with multi-agency approaches to CVE intervention.



s.13(1)(a)
s.15(1) - Int'l
s.16(1)(c)
s.21(1)(a)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Hostile State Activity (HSA) / Foreign Interference (FI)

Australia's approach to FI is whole-of-government, country-agnostic, with four pillars: transparency 'sunlight', enforcement, deterrence, and capability.

Initiatives undertaken include: instituting legislative reform; establishing strong cyber defences; and identifying vulnerabilities that could be exploited by malicious actors. In advance of its federal election on May 18, 2019, Australia established a multi-agency Electoral Integrity Assurance Taskforce, led by the Australian Electoral Commission, to manage risks and prepare the public for any threat to the integrity of the election, including malicious cyber activity, physical attack, electoral fraud and foreign interference.

The Taskforce worked with traditional and social media industries in the lead-up to the election, to ensure they were alert to issues like disinformation and removed content which not only contravened their own terms of service, but was non-compliant with Australian law or represented an act of foreign interference.

Prior to the election, Facebook announced that it would restrict advertisements from being purchased by non-Australians during the campaign. However, Facebook refused to introduce other political advertisement transparency features that have been introduced in countries such as the UK, the U.S. and India.

In February 2019, a 'sophisticated state actor' conducted a cyber-attack aimed at Australia's Parliament. Systems of the Liberal-National coalition and Labor parties were compromised. Australia did not publicly name or accuse any country suspected to have conducted the cyber-attack.

Canada is aware that Britain, France, and Germany have experienced foreign interference in recent elections. Canada passed the *Elections Modernization Act* (Bill C-76) to strengthen provisions against foreign interference, disinformation and foreign political spending during an election. It requires online advertising platforms, such as news or social media sites operating in Canada, to keep a registry of all political advertising they carry for at least two years after the publication date. Thus far, Google has responded by banning political advertising on its platforms during the election. Facebook has announced that it will establish a registry.

Canada has set up a Critical Election Incident Public Protocol (CEIPP) aimed at ensuring coherence and consistency in Canada's approach to publicly inform Canadians about incidents that threaten Canada's ability to have a free and fair election.

s.13(1)(a)
s.15(1) - Def
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Cyber Security

Protecting the Cyber Security of Critical Infrastructure

[redacted]

Australia's Telecommunications Sector Security Reforms (TSSR) program was reviewed in an effort to inform the development of Canada's Critical Cyber Systems initiative. The TSSR program places legal obligations to ensure the security and resilience of Australia's telecommunications infrastructure. This includes imposing a series of obligations on telecommunications services, including compliance with security requirements and mandatory reporting of changes to an organization's networks and systems. The program empowers the government to compel information to monitor and investigate compliance, as well as to issue directions to entities to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

National Cyber Security Action Plan

Canada's upcoming National Cyber Security Action Plan will serve as a blueprint for the implementation of the National Cyber Security Strategy (released June 2018). The Action Plan will outline initiatives and milestones supporting each of the Strategy's three goals (secure and resilient systems; an innovative and adaptive cyber ecosystem; and effective leadership, governance, and collaboration.

Fifth Generation (5G)

Australia has fully restricted from its 5G telecommunications any vendor who may be subject to extrajudicial directions from a foreign government that conflict with Australian law. If asked about Canada's position, you may wish to note to the Minister that, since 2013, the Communications Security Establishment (CSE)'s Security Review Program has been in place to help mitigate risks in Canadian 3G and 4G/LTE networks by testing and evaluating designated equipment and services [redacted] and excluding designated equipment from sensitive areas of Canadian networks.

Terrorist Listing

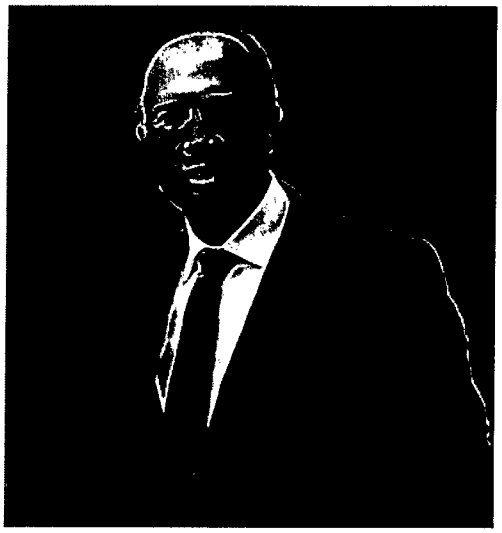
Canada is considering adding additional groups to its *Criminal Code* list of terrorist entities. As part of this process, you may wish to raise the prospect of listing an entity in concert with Australia.

Consulted: PACB/Canada Center and NCSB.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BIOGRAPHY

Peter Dutton – Minister for Home Affairs, Australia



Minister Dutton was appointed Minister for Home Affairs on December 20, 2017 upon the creation of the Department of Home Affairs. He has been a Member of Parliament for Dickson since 2001.

Minister Dutton's engagement in politics began in 1988, when he joined the Young Liberals, eventually becoming the chair of the Bayside Young Liberals. He graduated from the Queensland Police Academy in 1990 and subsequently worked as a police officer for nine years. He then attended Queensland University of Technology, obtaining a Bachelor of Business and founding Dutton Holdings along with his father.

Minister Dutton's first Ministerial appointment was in 2004, when he was appointed Minister for Workforce Participation. In 2006 he was promoted to Minister for Revenue and Assistant Treasurer. Following his re-election in 2007, and with the change of Government, he was promoted to Shadow Cabinet as Minister for Finance, Competition Policy and Deregulation. In 2008 he was promoted to the position of Shadow Minister for Health and Ageing.

In 2013, he was appointed as Minister for Health and Minister for Sport in the newly elected Abbott Government. In 2014, he was appointed as Minister for Immigration and Border Protection.

Department of Home Affairs:

The Minister for Home Affairs is responsible for the portfolio of the Australian Department of Home Affairs. The portfolio includes federal agencies such as the Australian Federal Police; Australian Border Force; and the Australian Security Intelligence Organization. The department's responsibilities include:

- National Security;
- Law enforcement;
- Emergency Management;
- Border Control;
- Immigration / refugees / citizenship; and
- Multicultural affairs.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Trump Says Huawei 5G Debate Poses 'No Problem' to U.S.-U.K. Ties

Margaret Talev and Justin Sink | Bloomberg | June 4, 2019

President Donald Trump said the U.S. and U.K. will be able to find common ground on Huawei Technologies Co., the Chinese telecom giant the U.S. has sought to bar from 5G networks, citing security concerns.

State visit of US President Donald J. Trump to United Kingdom

Donald Trump and Theresa May on June 4.Photographer: Neil Hall/Pool

"We are going to have absolutely an agreement on Huawei and everything else. We have an incredible intelligence relationship and we will be able to work out any differences," Trump said Tuesday during a joint press conference in London with British Prime Minister Theresa May. "This is a truly great ally and partner and we will have no problem with that."

The Trump administration is seeking to choke off Beijing's access to key technologies by limiting the sale of vital U.S. components to Huawei, claiming the equipment could enable China to spy on its users. The U.S. move requires American suppliers of Huawei, a crown jewel of Chinese manufacturing, to seek U.S. government permission to do business with the company.

The Trump administration has been leaning on allies to exclude Huawei from 5G networks. May's spokeswoman told reporters earlier Tuesday that the government is still reviewing its policy on Huawei and will make a decision based on "hard-headed technical assessments."

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

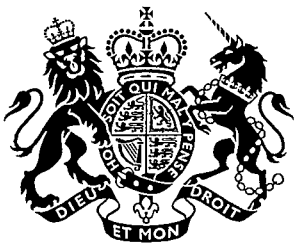
HM Government

Online Harms White Paper

April 2019

CP 57

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Online Harms White Paper

Presented to Parliament
by the Secretary of State for Digital, Culture, Media & Sport
and the Secretary of State for the Home Department
by Command of Her Majesty

April 2019

CP 57

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

© Crown copyright 2019

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gsi.gov.uk

ISBN 978-1-5286-1080-3
CCS0219683420 03/19

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Table of contents

Joint Ministerial foreword 3

Executive summary 5

PART 1: Introduction 11
1: The challenge 11
2: The harms in scope 30

PART 2: Regulatory model 41
3. A new regulatory framework 41
4: Companies in scope of the regulatory framework 49

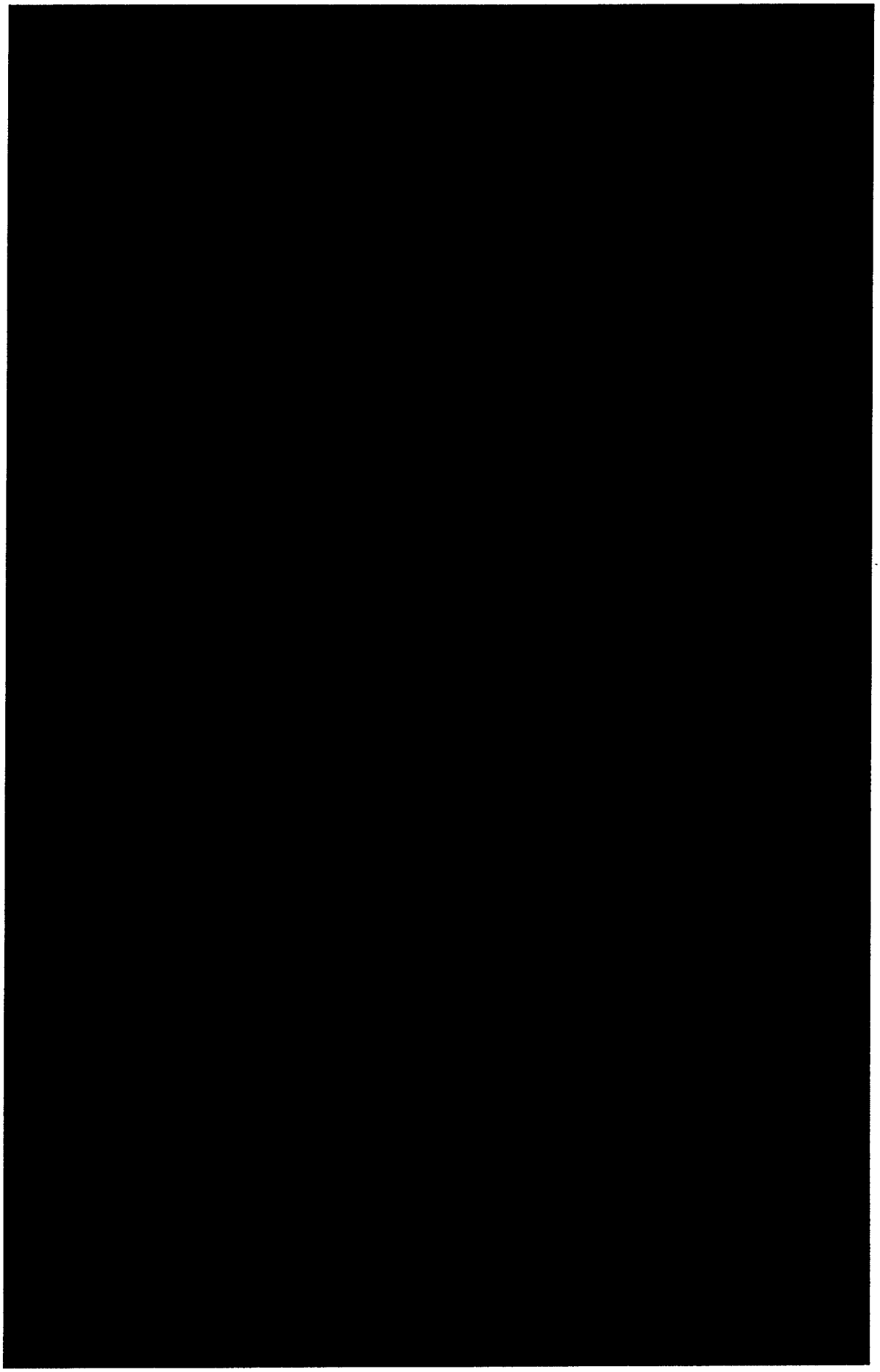
PART 3: Regulation in practice 53
5: A regulator for online safety 53
6: Enforcement 59
7. Fulfilling the duty of care 64

PART 4: Technology, education and awareness 77
8: Technology as part of the solution 77
9. Empowering users 85

Part 5: Conclusion and next steps 95
10: Conclusion and next steps 95

Annex A: How to respond to the consultation 97

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Joint Ministerial foreword





The internet is an integral part of everyday life for so many people. Nearly nine in ten UK adults and 99% of 12 to 15 year olds are online. As the internet continues to grow and transform our lives, often for the better, we should not ignore the very real harms which people face online every day.

In the wrong hands the internet can be used to spread terrorist and other illegal or harmful content, undermine civil discourse, and abuse or bully other people. Online harms are widespread and can have serious consequences.

Two thirds of adults in the UK are concerned about content online, and close to half say they have seen hateful content in the past year. The tragic recent events in New Zealand show just how quickly horrific terrorist and extremist content can spread online.

We cannot allow these harmful behaviours and content to undermine the significant benefits that the digital revolution can offer. While some companies have taken steps to improve safety on their platforms, progress has been too slow and inconsistent overall. If we surrender our online spaces to those who spread hate, abuse, fear and vitriolic content, then we will all lose.

So our challenge as a society is to help shape an internet that is open and vibrant but also protects its users from harm. The UK is committed to a free, open and secure internet, and will continue to protect freedom of expression online. We must also take decisive action to make people safer online.

This White Paper therefore puts forward ambitious plans for a new system of accountability and oversight for tech companies, moving far beyond self-regulation. A new regulatory framework for online safety will make clear companies' responsibilities to keep UK users, particularly children, safer online with the most robust action to counter illegal content and activity.

This will be overseen by an independent regulator which will set clear safety standards, backed up by reporting requirements and effective enforcement powers.

Although other countries have introduced regulation to address specific types of harm, this is the first attempt globally to address a comprehensive spectrum of online harms in a single and coherent way.

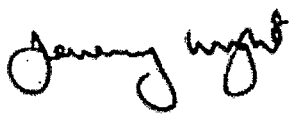
Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The UK's future prosperity will depend heavily on having a vibrant technology sector. Innovation and safety online are not mutually exclusive; through building trust in the digital economy and in new technologies, this White Paper will build a firmer foundation for this vital sector.

As a world-leader in emerging technologies and innovative regulation, the UK is well placed to seize these opportunities. We want technology itself to be part of the solution, and this White Paper proposes measures to boost the tech-safety sector in the UK, as well as measures to help users manage their safety online.

We believe the approach in this White Paper can lead towards new, global approaches for online safety that support our democratic values, and promote a free, open and secure internet; and we will work with other countries to build an international consensus behind it.

Online safety is a shared responsibility between companies, the government and users. We would encourage everyone to take part in the consultation that accompanies this White Paper, and work with us to make Britain the safest place in the world to be online.



Rt Hon Jeremy Wright MP
Secretary of State for Digital, Culture, Media and Sport



Rt Hon Sajid Javid MP
Home Secretary

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Executive summary

1. The government wants the UK to be the safest place in the world to go online, and the best place to start and grow a digital business. Given the prevalence of illegal and harmful content online, and the level of public concern about online harms, not just in the UK but worldwide, we believe that the digital economy urgently needs a new regulatory framework to improve our citizens' safety online. This will rebuild public confidence and set clear expectations of companies, allowing our citizens to enjoy more safely the benefits that online services offer.

The problem

2. Illegal and unacceptable content and activity is widespread online, and UK users are concerned about what they see and experience on the internet. The prevalence of the most serious illegal content and activity, which threatens our national security or the physical safety of children, is unacceptable. Online platforms can be a tool for abuse and bullying, and they can be used to undermine our democratic values and debate. The impact of harmful content and activity can be particularly damaging for children, and there are growing concerns about the potential impact on their mental health and wellbeing.
3. Terrorist groups use the internet to spread propaganda designed to radicalise vulnerable people, and distribute material designed to aid or abet terrorist attacks. There are also examples of terrorists broadcasting attacks live on social media. Child sex offenders use the internet to view and share child sexual abuse material, groom children online, and even live stream the sexual abuse of children.
4. There is also a real danger that hostile actors use online disinformation to undermine our democratic values and principles. Social media platforms use algorithms which can lead to 'echo chambers' or 'filter bubbles', where a user is presented with only one type of content instead of seeing a range of voices and opinions. This can promote disinformation by ensuring that users do not see rebuttals or other sources that may disagree and can also mean that users perceive a story to be far more widely believed than it really is.
5. Rival criminal gangs use social media to promote gang culture and incite violence. This, alongside the illegal sale of weapons to young people online, is a contributing factor to senseless violence, such as knife crime, on British streets.
6. Other online behaviours or content, even if they may not be illegal in all circumstances, can also cause serious harm. The internet can be used to harass, bully or intimidate, especially people in vulnerable groups or in public life. Young adults or children may be exposed to harmful content that relates, for example, to self-harm or suicide. These

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

experiences can have serious psychological and emotional impact. There are also emerging challenges about designed addiction to some digital services and excessive screen time.

Our response

7. This White Paper sets out a programme of action to tackle content or activity that harms individual users, particularly children, or threatens our way of life in the UK, either by undermining national security, or by undermining our shared rights, responsibilities and opportunities to foster integration.
8. There is currently a range of regulatory and voluntary initiatives aimed at addressing these problems, but these have not gone far or fast enough, or been consistent enough between different companies, to keep UK users safe online.
9. Many of our international partners are also developing new regulatory approaches to tackle online harms, but none has yet established a regulatory framework that tackles this range of online harms. The UK will be the first to do this, leading international efforts by setting a coherent, proportionate and effective approach that reflects our commitment to a free, open and secure internet.
10. As a world-leader in emerging technologies and innovative regulation, the UK is well placed to seize these opportunities. We want technology itself to be part of the solution, and we propose measures to boost the tech-safety sector in the UK, as well as measures to help users manage their safety online.
11. The UK has established a reputation for global leadership in advancing shared efforts to improve online safety. Tackling harmful content and activity online is one part of the UK's wider ambition to develop rules and norms for the internet, including protecting personal data, supporting competition in digital markets and promoting responsible digital design.
12. Our vision is for:
    - A free, open and secure internet.
    - Freedom of expression online.
    - An online environment where companies take effective steps to keep their users safe, and where criminal, terrorist and hostile foreign state activity is not left to contaminate the online space.
    - Rules and norms for the internet that discourage harmful behaviour.
    - The UK as a thriving digital economy, with a prosperous ecosystem of companies developing innovation in online safety.
    - Citizens who understand the risks of online activity, challenge unacceptable behaviours and know how to access help if they experience harm online, with children receiving extra protection.
    - A global coalition of countries all taking coordinated steps to keep their citizens safe online.
    - Renewed public confidence and trust in online companies and services.

Clarity for companies

13. Increasing public concern about online harms has prompted calls for further action from governments and tech companies. In particular, as the power and influence of large companies has grown, and privately-run platforms have become akin to public spaces,

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

some of these companies now acknowledge their responsibility to be guided by norms and rules developed by democratic societies.

14. The new regulatory framework this White Paper describes will set clear standards to help companies ensure safety of users while protecting freedom of expression, especially in the context of harmful content or activity that may not cross the criminal threshold but can be particularly damaging to children or other vulnerable users. It will promote a culture of continuous improvement among companies, and encourage them to develop and share new technological solutions rather than complying with minimum requirements.
15. It will also provide clarity for the wide range of businesses of all sizes that are in scope of the new regulatory framework but whose services present much lower risks of harm, helping them to understand and fulfil their obligations in a proportionate manner.

A new regulatory framework for online safety

16. The government will establish a new statutory duty of care to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services.
17. Compliance with this duty of care will be overseen and enforced by an independent regulator.
18. All companies in scope of the regulatory framework will need to be able to show that they are fulfilling their duty of care. Relevant terms and conditions will be required to be sufficiently clear and accessible, including to children and other vulnerable users. The regulator will assess how effectively these terms are enforced as part of any regulatory action.
19. The regulator will have a suite of powers to take effective enforcement action against companies that have breached their statutory duty of care. This may include the powers to issue substantial fines and to impose liability on individual members of senior management.
20. Companies must fulfil the new legal duty. The regulator will set out how to do this in codes of practice. If companies want to fulfil this duty in a manner not set out in the codes, they will have to explain and justify to the regulator how their alternative approach will effectively deliver the same or greater level of impact.
21. Reflecting the threat to national security or the physical safety of children, the government will have the power to direct the regulator in relation to codes of practice on terrorist activity or child sexual exploitation and abuse (CSEA) online, and these codes must be signed off by the Home Secretary.
22. For codes of practice relating to illegal harms, including incitement of violence and the sale of illegal goods and services such as weapons, there will be a clear expectation that the regulator will work with law enforcement to ensure the codes adequately keep pace with the threat.
23. Developing a culture of transparency, trust and accountability will be a critical element of the new regulatory framework. The regulator will have the power to require annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms and what countermeasures they are taking to address these. These reports will be published online by the regulator, so that users and parents can make informed decisions about internet use. The regulator will also have powers to require additional information, including about the impact of algorithms in selecting

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

content for users and to ensure that companies proactively report on both emerging and known harms.

24. The regulator will encourage and oversee the fulfilment of companies' existing commitments to improve the ability of independent researchers to access their data, subject to appropriate safeguards.

25. As part of the new duty of care, we will expect companies, where appropriate, to have effective and easy-to-access user complaints functions, which will be overseen by the regulator. Companies will need to respond to users' complaints within an appropriate timeframe and to take action consistent with the expectations set out in the regulatory framework.

26. We also recognise the importance of an independent review mechanism to ensure that users have confidence that their concerns are being treated fairly. We are consulting on options, including allowing designated bodies to make 'super complaints' to the regulator in order to defend the needs of users.

27. Ahead of the implementation of the new regulatory framework, we will continue to encourage companies to take early action to address online harms. To assist this process, this White Paper sets out high-level expectations of companies, including some specific expectations in relation to certain harms. We expect the regulator to reflect these in future codes of practice.

28. For the most serious online offending such as CSEA and terrorism, we will expect companies to go much further and demonstrate the steps taken to combat the dissemination of associated content and illegal behaviours. We will publish interim codes of practice, providing guidance about tackling terrorist activity and online CSEA later this year.

The companies in scope of the regulatory framework

29. We propose that the regulatory framework should apply to companies that allow users to share or discover user-generated content or interact with each other online.

30. These services are offered by a very wide range of companies of all sizes, including social media platforms, file hosting sites, public discussion forums, messaging services and search engines.

31. The regulator will take a risk-based and proportionate approach across this broad range of business types. This will mean that the regulator's initial focus will be on those companies that pose the biggest and clearest risk of harm to users, either because of the scale of the platforms or because of known issues with serious harms.

32. Every company within scope will need to fulfil their duty of care, particularly to counter illegal content and activity, comply with information requests from the regulator, and, where appropriate, establish and maintain a complaints and appeals function which meets the requirements to be set out by the regulator.

33. Reflecting the importance of privacy, any requirements to scan or monitor content for tightly defined categories of illegal content will not apply to private channels. We are consulting on definitions of private communications, and what measures should apply to these services.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

An independent regulator for online safety

34. An independent regulator will implement, oversee and enforce the new regulatory framework. It will have sufficient resources and the right expertise and capability to perform its role effectively.

35. The regulator will take a risk-based approach, prioritising action to tackle activity or content where there is the greatest evidence or threat of harm, or where children or other vulnerable users are at risk. To support this, the regulator will work closely with UK Research and Innovation (UKRI) and other partners to improve the evidence base. The regulator will set out expectations for companies to do what is reasonably practicable to counter harmful activity or content, depending on the nature of the harm, the risk of the harm occurring on their services, and the resources and technology available to them.

36. The regulator will have a legal duty to pay due regard to innovation, and to protect users' rights online, taking particular care not to infringe privacy or freedom of expression. We are clear that the regulator will not be responsible for policing truth and accuracy online.

37. The government is consulting on whether the regulator should be a new or existing body. The regulator will be funded by industry in the medium term, and the government is exploring options such as fees, charges or a levy to put it on a sustainable footing. This could fund the full range of the regulator's activity, including producing codes of practice, enforcing the duty of care, preparing transparency reports, and any education and awareness activities undertaken by the regulator.

Enforcement of the regulatory framework

38. The regulator will have a range of enforcement powers, including the power to levy substantial fines, that will ensure that all companies in scope of the regulatory framework fulfil their duty of care.

39. We are consulting on which enforcement powers the regulator should have at its disposal, particularly to ensure a level playing field between companies that have a legal presence in the UK, and those which operate entirely from overseas.

40. In particular, we are consulting on powers that would enable the regulator to disrupt the business activities of a non-compliant company, measures to impose liability on individual members of senior management, and measures to block non-compliant services.

41. The new regulatory framework will increase the responsibility of online services in a way that is compatible with the EU's e-Commerce Directive, which limits their liability for illegal content until they have knowledge of its existence, and have failed to remove it from their services in good time.

Technology as part of the solution

42. Companies should invest in the development of safety technologies to reduce the burden on users to stay safe online.

43. In November 2018, the Home Secretary co-hosted a hackathon with five major tech companies to develop a new tool to tackle online grooming, which will be licensed for free to other companies, but more of these innovative and collaborative efforts are needed.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

44. The government and the regulator will work with leading industry bodies and other regulators to support innovation and growth in this area and encourage the adoption of safety technologies.

45. The government will also work with industry and civil society to develop a safety by design framework, linking up with existing legal obligations around data protection by design and secure by design principles, to make it easier for start-ups and small businesses to embed safety during the development or update of products and services.

Empowering users

46. Users want to be empowered to keep themselves and their children safe online, but currently there is insufficient support in place and many feel vulnerable online.

47. While companies are supporting a range of positive initiatives, there is insufficient transparency about the level of investment and the effectiveness of different interventions. The regulator will have oversight of this investment.

48. The government will develop a new online media literacy strategy. This will be developed in broad consultation with stakeholders, including major digital, broadcast and news media organisations, the education sector, researchers and civil society. This strategy will ensure a coordinated and strategic approach to online media literacy education and awareness for children, young people and adults.

Next steps

49. This is a complex and novel area for public policy. To this end, as well as setting out the government's proposed approach, this White Paper poses a series of questions about the design of the new regulatory framework and non-legislative package. A full list of these questions is included at the end of this White Paper.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

PART 1: Introduction

1: The challenge

Summary

- Illegal and unacceptable content and activity is widespread online, and UK users are frequently concerned about what they have seen or experienced.
- The prevalence of the most serious illegal content and activity on the internet, which threatens our national security or the physical safety of children, is unacceptable. The ease and extremity of the most serious online offending such as child sexual exploitation and abuse (CSEA) continues to increase.
- The impact of harmful content and activity can be particularly damaging for children and young people, and there are growing concerns about the potential impact on their mental health and wellbeing.
- Tackling illegal and harmful content and activity online is one part of the UK's wider mission to develop rules and norms for the internet, including protecting personal data, supporting competition in digital markets and promoting responsible digital design.

1.1 The internet is an integral part of everyday life for so many people. Nearly nine in ten UK adults are online and adult users spend around one day a week on the internet.[1] This is also true for children and young people, with 99% of 12-15 year olds going online, spending an average of twenty and a half hours a week on the internet.[2]

1.2 The internet can be a powerful force for good. It serves humanity, spreads ideas and enhances freedom and opportunity across the world. Online services facilitate the exchange of information, goods and services. They match supply and demand with great efficiency, increase consumer choice and lower distance between participants.

1 Ofcom (2018). Adults' Media Use and Attitudes Report. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf

2 Ofcom (2018). Children and parents: media use and attitudes report 2018. Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1.3 However, there is growing evidence of the scale of harmful content and activity that people experience online. Online services can be used to spread terrorist propaganda and child abuse content, they can be a tool for abuse and bullying, and they can be used to undermine civil discourse. Despite the many benefits of the internet, more than one in four adult users in the UK have experienced some form of harm related either to content or interactions online.[3]

1.4 Social media platforms and other technology companies increasingly acknowledge that they have a greater responsibility to protect their users from harm. British citizens want to feel empowered to keep themselves and their children safe and secure online. Both the government and industry have a responsibility to ensure this is the case.

Online harms suffered by individuals

1.5 The most appalling and horrifying illegal content and activity remains prevalent on an unacceptable scale. Existing efforts to tackle this activity have not delivered the necessary improvements, creating an urgent need for government to intervene to drive online services to step up their response.

1.6 There is a growing threat presented by online CSEA. In 2018 there were over 18.4 million referrals of child sexual abuse material by US tech companies to the National Center for Missing and Exploited Children (NCMEC).[4] Of those, there were 113, 948 UK-related referrals in 2018, up from 82,109 in 2017. In the third quarter of 2018, Facebook reported removing 8.7 million pieces of content globally for breaching policies on child nudity and sexual exploitation.[5]

1.7 Not only is the scale of this offending increasing, so is its severity. The internet Watch Foundation (IWF) estimates that 55% of the child sexual abuse material they find online contains children aged ten or under, and 33% of this imagery is in the most serious category of abuse.[6]

1.8 Terrorists also continue to use online services to spread their vile propaganda and mobilise support (see Box 2). Terrorist content online threatens the UK's national security and the safety of the public.

1.9 All five terrorist attacks in the UK during 2017 had an online element, and online terrorist content remains a feature of contemporary radicalisation.[7] It is seen across terrorist investigations, including cases where suspects have become very quickly radicalised to the point of planning attacks. This is partly as a result of the continued availability and deliberately attractive format of the terrorist material they are accessing online.

1.10 Terrorist groups work to find new ways to spread their propaganda and evade government and law enforcement efforts to prevent this. These threats are not only restricted to the largest, best-known services, but are prevalent across the internet. Terrorist groups and their supporters constantly diversify their reliance on the online services they use to host their

3 Ofcom and ICO (2018). Internet users' experience of harm online 2018. Available at: https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-of-harm-online

4 NCMEC. Available at: http://www.missingkids.com/footer/media/vnr/vnr2

5 Facebook (2018). Transparency Report. Available at: https://transparency.facebook.com/community-standards-enforcement#child-nudity-and-sexual-exploitation

6 Internet Watch Foundation (2017). Annual Report 2017. Available at: https://annualreport.iwf.org.uk/

7 Speech at Digital Forum, San Francisco by the Rt Hon Amber Rudd, 13 February 2018.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

material online. While Facebook reported removing over 14 million pieces of content related to terrorism or violent extremism in 2018,[8] the terrorist group Daesh used over 100 platforms in 2018, making use of a wider range of more permissive and smaller platforms.

1.11 We have also seen terrorists and their supporters adopting new techniques, with material being shared using hacked social media accounts, and propaganda videos being edited in an effort to avoid detection.

1.12 Terrorist groups place a huge premium on quickly reaching their audiences. A third of all links to Daesh propaganda, for example, are disseminated within an hour of upload, while in the immediate aftermath of the terrorist attack in Christchurch, there was a co-ordinated cross-platform effort to generate maximum reach of footage of the attack. It is therefore vital to ensure that there is the technology in place to automatically detect and remove terrorist content within an hour of upload, secure the prevention of re-upload and prevent, where possible, new content being made available to users at all.

1.13 The threat continues to evolve with terrorists' relentless desire to seek out new ways to share their propaganda in an effort to radicalise and recruit. The most effective way to combat this adaptive threat is to have a consistent cross-platform response to ensure there are no safe spaces for terrorists to operate online.

1.14 Rival gangs use social media to glamourise weapons and gang life, as well as to directly depict or incite acts of violence. Alongside the illegal sale of weapons to young people online, this is a contributing factor to incidents of serious violence, including knife crime, in the UK. The latest police recorded crime figures, for the year ending September 2018, show an 8% increase in knife crime (to 39,818 offences) compared with the previous year. Homicide figures have risen by 14% (excluding terrorist attacks) over the same period.[9]

Harm: Child sexual exploitation and abuse online **Box 1**

Threat:

Child sex offenders use the internet to view and share Child Sexual Abuse Material (CSAM), groom children online, and live stream the sexual abuse of children. The sheer scale of CSEA online is horrifying.

- In 2017, the IWF assessed 80,319 confirmed reports of websites hosting or linking to images of child sexual abuse. A total of 43% of the children in the images were aged 11-15 years old, and 57% were ten years old or younger. Two per cent were aged two or younger.[10]
- Sexual exploitation can happen to any young person – whatever their background, age, gender, race or sexuality or wherever they live.
- In the most horrific cases, child sex offenders in developing countries are abusing children at the instigation of offenders in the UK who commission the abuse online and watch it over live stream for a fee.

8 Facebook (2018). Transparency Report. Available at: https://transparency.facebook.com/community-standards-enforcement#child-nudity-and-sexual-exploitation

9 ONS (2019). Crime in England and Wales, Year Ending September 2018. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018

10 Internet Watch Foundation (2017). Annual Report 2017. Available at: https://annualreport.iwf.org.uk/

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Impact:

- Victims of abuse report ongoing trauma caused by the knowledge that images of their abuse are still being circulated and viewed by child sex offenders online. Victims also fear being recognised as a result of their images being available online.
- Victims of online grooming suffer lasting harm after being blackmailed and coerced into sharing indecent images of themselves or live-streaming themselves to offenders, and live in fear that those images could be used against them.

Harm: Terrorist content online **Box 2**

Threat:

Terrorists, including Islamist groups such as Daesh and Al-Qaeda as well as far right terrorists, use the internet to spread propaganda designed to radicalise vulnerable people, and distribute material designed to aid and abet terrorist attacks. There are also examples of terrorists broadcasting attacks live on social media. Terrorist use of the internet poses a threat to national security and the safety of the public.

- As larger platforms take more action against terrorist propaganda, terrorist groups have spread out to a wider range of more permissive and smaller platforms.
- Terrorist groups are adopting new techniques to avoid detection, including sharing material via hacked social media accounts, and subtly altering propaganda videos.
- Terrorist groups place a huge premium on quickly reaching their audiences.

Impact:

- The availability and spread of terrorist content online has been shown to contribute to terrorist attacks on UK soil.
- All five of the terrorist attacks undertaken in the UK during 2017 had an online element to them.[11]
- Online terrorist content is seen across terrorist investigations, including cases where suspects have become very quickly radicalised to the point of planning attacks.

11 Speech at Digital Forum (2018). San Francisco by the Rt Hon Amber Rudd, 13 February 2018

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Harm: Content illegally uploaded from prisons **Box 3**

Threat:

There are an increasing number of cases where online content originating from prisons is illegally uploaded by prisoners to social media.

- Some prisoners transmit videos, images and messages from prisons using prohibited devices such as mobile phones.
- They can use social media accounts to harass and intimidate their victims.

Impact:

- This can lead to victims of crime feeling that they have no escape from their tormentors, even when they have been imprisoned.
- Prisoners openly uploading content from prisons can also undermine public confidence in the prison service.

Tackling serious violence online **Box 4**

Rival gangs use social media to promote gang culture, taunt each other and incite violence. Content can also either directly depict or incite real world violence or glamourise gang life and the use of weapons. Government and law enforcement are taking action to tackle this threat:

- We have provided £1.4 million to support a new national police capability to tackle gang related activity on social media.
- This will bring together a dedicated team to take action against online material, focusing on investigative, disruption and enforcement work against specific gang targets, as well as making referrals to social media companies so illegal and harmful content can be taken down.
- Prior to this, a new action group was established to bring together government, social media companies, police and community groups to tackle violent material available via social media.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Harm: The sale of opioids online **Box 5**

Threat:

Powerful and dangerous opioids are marketed and sold online. Fentanyl and its analogues (substances with similar but slightly altered chemical structures) are a group of powerful synthetic opioids. They have similar effects to other opioids such as morphine and heroin, but are significantly more potent.

- Since December 2016, there have been at least 143 recorded deaths in the UK attributed to Fentanyl and its analogues.[12] Fentanyl has been sold on several well-known social media sites. The products are marketed as top-quality substances with fast and secure delivery, with mobile phone numbers provided for follow-up contact.[13]
- Of particular concern is that some social media groups and threads, including those used by vulnerable people, are being targeted. This includes people suffering from chronic pain, where there is a risk of accidental overdose and people dealing with depression, where there is a risk that the fentanyl may be used to assist suicide.

Impact:

- Whilst these products continue to be made available there is a risk that fatalities will increase.
- There is also a risk that health professionals and other first responders will continue to be exposed to potentially harmful environments.

1.15 Beyond illegal activity, other behaviour online also causes harm. In 2017, one in five children aged 11 to 19 reported having experienced cyberbullying in the past year[14]; 21% of women have received misogynistic abuse online,[15] and half of girls aware of sexist abuse on social media say this has restricted what they do or aspire to in some way.[16] The House of Commons Petitions Committee has highlighted the extreme abuse experienced online by disabled people, which has forced some of them to leave social media.[17]

1.16 Victims have also described a qualitative difference between online and offline harms, particularly in reference to online abuse. The Law Commission noted the perceived anonymity of offenders as one of the characteristics of online abuse that may result in a different experience for victims – see Box 6.[18] Many users also feel that the market currently offers

12 NCA analysis.
13 Ibid.
14 NHS Digital (2018). Mental Health of Children and Young People in England, 2017. Available at: https://files.digital.nhs.uk/C9/999365/MHCYP%202017%20Behaviours%20Lifestyles%20Identities.pdf
15 Amnesty International (2017). The impact of online abuse against women. Available at: https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/
16 Girl Guiding (2016). Girls Attitudes Survey 2016. Available at: https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2016.pdf
17 House of Commons Petitions Committee (2019). Online abuse and the experience of disabled people. The Petitions Committee, 2019. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmpetitions/759/759.pdf
18 Law Commission (2018). Abusive and Offensive Communications. Available at: https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

them very few alternative, safer online services. For example, the 2018 Doteveryone Digital Attitudes[19] report found that almost half of respondents felt they had no choice but to sign up to online services, even where they had concerns.

Tackling online anonymous abuse **Box 6**

The internet can be used to harass, bully or intimidate. In many cases of harassment and other forms of abusive communications online, the offender will be unknown to the victim. In some instances, they will have taken technical steps to conceal their identity. Government and law enforcement are taking action to tackle this threat.

- The police have a range of legal powers to identify individuals who attempt to use anonymity to escape sanctions for online abuse, where the activity is illegal. The government will work with law enforcement to review whether the current powers are sufficient to tackle anonymous abuse online.
- We are enhancing law enforcement's ability to tackle anonymous online abuse by investing in training that is designed to improve digital capability across policing. For example, as part of the £46 million Police Transformation Fund allocated by the Home Office, the Digital Investigation and Intelligence programme will build police capability to respond to the full range of digital crime types, through investment in technology and training.
- We are also making it easier for the public to report online crimes. Through the Digital Public Contact programme, we will provide the public with a digitally accessible police force with a consistent set of online capabilities to use in engaging and transacting with police services through a single online channel.
- We also expect companies to do substantially more to keep their users safe and counter online abuse, particularly where this is illegal. Companies need to take responsibility for tackling abusive behaviour on their services. More detail is set out in Chapter 3.

Online harms suffered by children and young people

1.17 Being online can be a hugely positive experience for children and young people – see Box 7. Recent research by internet Matters found that seven in ten parents think screen time is essential for their children's learning development and two thirds of parents feel that devices give their children another outlet for creativity, particularly so for children aged 6-10.[20]

1.18 However, the impact of harmful content and activity can be particularly damaging for children, as set out in Box 1 above and Boxes 8-10 below. There is also growing concern about the relationship between social media and the mental health of children and young people. The Children's Commissioner's report published in November 2018 *Who knows what about me* sets out the huge size and growth of children's digital footprint and the associated

19 Doteveryone (2018). People, Power and Technology: The 2018 Digital Attitudes Report. Available at: https://attitudes.doteveryone.org.uk/files/People%20Power%20and%20Technology%20Doteveryone%20Digital%20Attitudes%20Report%202018.pdf

20 Internet Matters (2018). Look Both Ways: Practical Parenting in the Age of Screens. Available at: https://www.internetmatters.org/about-us/screen-time-report-2018/

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

risks and benefits.[21] Internet Matters reported in February 2019 that vulnerable young people are more likely to suffer online harms and less likely to receive online safety advice and education.[22]

The positive impact of being online for children and young people **Box 7**

Most children have a positive experience online, using the internet for social networking and connecting with peers, as well as to access educational resources, information, and entertainment. The internet opens up new opportunities for learning, performance, creativity and expression.

- A literature review by the UK Council for Child Internet Safety (2017) highlights evidence that young people recognise the positive role of the internet in relation to self-expression, developing understanding, bringing people together and respecting and celebrating differences.[23] Research by UNICEF (2017) shows that use of technology is beneficial for children's social relationships, enabling them to enhance existing relationships and build positive friendships online.[24]
- A report by The Royal Society for Public Health in 2017 found that young people reading blogs or watching vlogs on personal health issues helped improve their knowledge and understanding, prompted individuals to access health services, and enabled them to better explain their own health issues or make better choices.[25] They also found that young people are increasingly turning to social media as a means of emotional support to prevent and address mental health issues.
- More recently, research by Ofcom showed that nine in ten social media users aged 12-15 state that this use has made them feel happy or helped them feel closer to their friends. Two thirds of 12-15 year olds who use social media or messaging sites say they send support messages, comments or posts to friends if they are having a difficult time. One in eight support causes or organisations by sharing or commenting on posts.[26]
- In the 2019 UK Safer Internet Centre survey,[27] 70% of young people surveyed said that being online helps them understand what's happening in the world, with 60% noting they have only seen or heard about certain issues or news because they heard about them from the internet. 43% said they have been inspired to take action because of something they saw online, with 48% stating being online makes them feel that their voice or actions matter.

21 Children's Commissioner (2018). Who knows what about me? Available at: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/who-knows-what-about-me.pdf

22 Internet Matters (2019). Vulnerable Children in a Digital World. Available at: https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/Vulnerable-Children-in-a-Digital-World-FINAL.pdf

23 UKCCIS Evidence Group (2017). Children's online activities, risks and safety. Available at: https://www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group

24 UNICEF (2017). How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? Available at: https://www.unicef-irc.org/publications/pdf/Children-digital-technology-wellbeing.pdf

25 RSPH (2017). Status of mind: Social media and young people's mental health and wellbeing. Available at: https://www.rsph.org.uk/uploads/assets/uploaded/62be270a-a55f-4719-ad668c2ec7a74c2a.pdf

26 Ofcom (2018). Children and parents: media use and attitudes report 2018. Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018

27 UK Safer Internet Centre (2019). Our internet, Our Choice Report. Available at: https://www.saferInternet.org.uk/safer-Internet-day/safer-Internet-day-2019/our-Internet-our-choice-report

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Harm: Cyberbullying **Box 8**

Threat:

In 2017, one in five children surveyed aged 11-19 reported having experienced cyberbullying in the past year.[28]

- The prevalence of cyberbullying is higher for some groups, such as women, religious minorities, LGBT+, BME and disabled individuals.[29]

Impact:

- Cyberbullying has been shown to have psychological and emotional impact. In a large survey of young people who had been cyberbullied, 41% had developed social anxiety, 37% had developed depression, 26% had suicidal thoughts and 25% had self-harmed.[30]
- These figures are all higher than corresponding statistics for 'offline' bullying, and indicated the increased potential for harm of cyberbullying.

Harm: Self-harm and suicide **Box 9**

Threat:

In a survey of young adults, 22.5% reported self-harm and suicide-related internet use, including 8.2% and 7.5% who had actively searched for information about self-harm and suicide respectively.[31]

- Amongst those who had harmed with suicidal intent, 70% reported self-harm and suicide-related internet use.[32]
- The prevalence of using the internet to view related content has also been found to be higher in children than adults. One study of those presenting to hospital following self-harm found that 26% of children had viewed self-harm and suicide content, compared to 8.4% of adults.[33]

28 NHS Digital (2018). Mental Health of Children and Young People in England, 2017. Available at: https://files.digital.nhs.uk/C9/999365/MHCYP%202017%20Behaviours%20Lifestyles%20Identities.pdf

29 Ditch the Label (2017). 'The Annual Bullying Survey 2017'. Available at: https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-2.pdf

30 Ibid.

31 Mars, B et al. (2015). Exposure to, and searching for, information about suicide and self-harm on the internet: Prevalence and predictors in a population based cohort of young adults' Journal of affective disorders,185, 239-45. Available at: https://doi.org/10.1016/j.jad.2015.06.001

32 Ibid.

33 Padmanathan, P. et al. (2018). Suicide and Self-Harm Related internet Use. Crisis. Available at: https://doi.org/10.1027/0227-5910/a000522

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Impact

- The National Confidential Inquiry into Suicide and Safety in Mental Health (NCISH) analysed the characteristics of 595 children and young people (aged under 20) who had died by suicide in the UK between 2014 and 2016.
- The NCISH found that suicide-related internet use (i.e. searching the internet for information on suicide methods) was reported for almost a quarter (23%) of these children and young people.[34]

Harm: Underage sharing of sexual imagery **Box 10**

Many children and young people take and share sexual images. Creating, possessing, copying or distributing sexual or indecent images of children and young people under the age of 18 is illegal, including those taken and shared by the subject of the image.

- Surveys provide tentative evidence that between 26%[35] and 38%[36] of 14-17 year olds have sent sexual images to a partner, and between 12% and 49% have received a sexual image.[37]
- The proportion of young people sending images varies with age, with one study indicating that 26% of 14 year olds had sent and received sexual images, rising to 48% of 16 year olds.[38]

Impact

- Sharing sexual images can expose children and young people to bullying, humiliation, objectification and guilt. These images can be shared widely and appear on offender forums or adult pornography sites, or be used to extort further imagery. This puts children and young people in a vulnerable position and at risk of harm. It is a criminal offence to produce, possess or share sexual images of under 18 year olds.
- The National Society for the Prevention of Cruelty to Children (NSPCC) reported that sexting was discussed in 1,392 counselling sessions with children and young people on their helplines that year, representing a 15% increase on the year before.[39]

1.19 The UK Chief Medical Officers (UK CMOs) commissioned independent researchers to carry out a systematic evidence review on the impact of social media use on children and young people's mental health. The review covered important and diverse issues including cyberbullying, online gaming, sleep problems and problematic internet use, which is also known as 'internet addiction'.

34 National Confidential Inquiry into Suicide and Safety in Mental Health (2018). Annual Report: England, Northern Ireland, Scotland, Wales. University of Manchester. Available at: http://documents.manchester.ac.uk/display.aspx?DocID=38469

35 Brook (2017). Digital Romance. Available at: https://www.brook.org.uk/press-releases/digital-romance

36 UKCCIS Evidence Group (2017). Children's online activities, risks and safety. Available at: https://www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group

37 Ibid.

38 Ibid.

39 Ibid.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1.20 Overall the research did not present evidence of a causal relationship between screen-based activities and mental health problems, but it did find some associations between screen-based activities and negative effects, such as increased risk of anxiety or depression.[40] It is important that parents and carers support their children to have positive experiences online.

1.21 While there is not yet sufficient evidence about the impact of screen time to support detailed guidelines for parents or requirements on companies, we will continue to support research in this area and ensure high quality advice is available to families. We also welcome efforts from the industry to develop tools to help individuals and families understand and manage how much time they spend online – more information on these is in Box 33.

Emerging challenge: Screen time **Box 11**

Screen time and its impact on children is an issue of growing concern. Research by Internet Matters found that nearly half of parents (47%) are concerned about the amount of time their child spends online and 88% take measures to limit their child's use of devices.[41]

- The UK CMOs recently conducted a systematic evidence review on children and young people's screen and social media use. The CMO subsequently produced advice for parents and carers to encourage them to discuss boundaries with children around online behaviours and time spent using screens, and to lead by example.
- For example, the UK CMOs advised that:
  - Sleep matters. Getting enough good quality sleep is very important. Leave phones outside the bedroom when it is bedtime.
  - Sharing sensibly. Talk about sharing photos and information online and how photos and words are sometimes manipulated. Parents and carers should never assume that children are happy for their photos to be shared. For everyone – when in doubt, don't upload!
  - Education matters. Make sure you and your children are aware of, and abide by, their school's policy on screen time.
  - Keep moving! Everyone should take a break after a couple of hours sitting or lying down using a screen. It's good to get up and move about a bit. #sitlessmovemore
  - Safety when out and about. Advise children to put their screens away while crossing the road or doing an activity that needs their full attention.
  - Talking helps. Talk with children about using screens and what they are watching. A change in behaviour can be a sign they are distressed – make sure they know they can always speak to you or another responsible adult if they feel uncomfortable with screen or social media use.

40 Department of Health and Social Care (2019). United Kingdom Chief Medical Officers' commentary on Screen-based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews. Available at: https://www.gov.uk/government/publications/uk-cmo-commentary-on-screen-time-and-social-media-map-of-reviews

41 Internet Matters (2018). Look Both Ways: Practical Parenting in the Age of Screens. Available at: https://www.internetmatters.org/about-us/screen-time-report-2018/

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Family time together. Screen-free meal times are a good idea – you can enjoy face-to-face conversation, with adults giving their full attention to children.
- Use helpful phone features. Some devices and platforms have special features – try using these features to keep track of how much time you (and, with their permission, your children) spend looking at screens or on social media.

Future action – building our understanding

Given the amount of time many children spend online, and the level of parental concern on this issue, we urgently need to build a better understanding.

- While we do not expect the regulator to set requirements around screen time, both government and the regulator will continue to support research in this area to inform future action in this space.
- We need to develop a better understanding of not just of the impact of screen time as a whole, but also between different types of screen time and children's development and wellbeing.
- As part of this, we also expect companies to support the developing evidence base around screen time, for example by providing access to anonymised data to researchers as recommended by the CMOs.
- If the emerging evidence base demonstrates a strong link between different elements of screen time and damage to children's wellbeing or development, companies will be expected to take appropriate action to fulfil their duty of care.

Threats to our way of life

1.22 The UK's reputation and influence across the globe is founded upon our values and principles. Our society is built on confidence in public institutions, trust in electoral processes, a robust, lively and plural media, and hard-won democratic freedoms that allow different voices, views and opinions to freely and peacefully contribute to public discourse.

1.23 Inaccurate information, regardless of intent, can be harmful – for example the spread of inaccurate anti-vaccination messaging online poses a risk to public health. The government is particularly worried about disinformation (information which is created or disseminated with the deliberate intent to mislead; this could be to cause harm, or for personal, political or financial gain).

1.24 Disinformation threatens these values and principles, and can threaten public safety, undermine national security, fracture community cohesion and reduce trust.

1.25 These concerns have been well set out in the wide-ranging inquiry led by the Digital, Culture, Media and Sport (DCMS) Select Committee report on fake news and disinformation, published on 18 February 2019. This White Paper has benefited greatly from this analysis and takes forward a number of the recommendations. The government will be responding to the DCMS Select Committee report in full in due course. We also note the recent papers from the Electoral Commission and Information Commissioner's Office on this and wider issues, and are considering these closely.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Harm: Online disinformation **Box 12**

Threat:

Online disinformation – spreading false information to deceive deliberately – is becoming more and more prevalent. Misinformation refers to the inadvertent sharing of false information.

- A recent study from the University of Oxford's Computational Propaganda Project has found evidence of organised social media manipulation campaigns in 48 countries in 2018.[42] According to the Reuters Institute, 61% of people want the government to do more to separate what is real and fake on the internet (2018).[43]
- One of the major technological challenges in disinformation is the continued development of AI systems. AI techniques can be used to target and manipulate individual voters, with highly sophisticated micro-targeting based on individual psychology.
- AI can be beneficial in the automatic detection of content, or automatically fact-checking articles. But developments in AI also make it possible to generate fake content (text, audio and video) which is difficult to detect by humans and algorithms – known as 'deepfakes'. As a result, it is becoming even easier to create and disseminate false content and narratives.
- The Russian State is a major source of disinformation. The Kremlin has used disinformation to obfuscate and confuse audiences around their illegal annexation of Crimea, intervention in eastern Ukraine and the shooting down of Malaysian Airlines flight MH17, which led to the deaths of 298 people including ten UK citizens. After the attempted murder of Sergei and Yulia Skripal in Salisbury in March 2018, the Russian State led a concerted disinformation campaign to distract from their culpability. This included the use of state media and covert social media accounts to sow over 40 different narratives as to what happened.

Impact:

- Most users are not always aware that much of the content they see is determined by sophisticated algorithms that draw on data about their online activity, such as their browsing history, their social media networks and what they post.
- Research by Doteveryone suggests that 62% of people do not realise that their social networks can affect the news they see,[44] while only three in ten adult online users questioned by Ofcom were aware of the ways in which companies can collect data about them online.[45]

42 Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation.Available at: https://comprop.oii.ox.ac.uk/research/cybertroops2018/

43 Newman, N. et al. (2018). Reuters Institute Digital News Report 2018. Available at: http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475

44 Miller, C., Coldicutt, R., and Kitcher, H. (2018). People, Power and Technology: The 2018 Digital Understanding Report Doteveryone. Available at: http://understanding.doteveryone.org.uk/files/Doteveryone_PeoplePowerTechDigitalUnderstanding2018.pdf

45 Ofcom (2018). Adults' Media Use and Attitudes Report. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Harm: Online manipulation **Box 13**

Threat:

Propaganda and false information have long been used to persuade and mislead, but the internet, social media and AI provide ever more effective ways to manipulate opinion.

- The tolerance of conflicting views and ideas are core facets of our democracy. However, these are inherently vulnerable to the efforts of a few to manipulate and confuse the information environment for nefarious purposes, including undermining trust. A combination of personal data collection, AI based algorithms and false or misleading information could be used to manipulate the public with unprecedented effectiveness.
- The distinction between legitimate influence and illegitimate manipulation is not new. The government took action to prevent subliminal broadcast advertising in the Broadcasting Act 1990. The government gave the Independent Television Commission (replaced by Ofcom) a duty to ensure that licensed services complied with requirements not to include technical devices which convey messages or influence individuals without them being aware. We believe the government should make sure there are similar boundaries between legitimate and illegitimate practices online. The techniques and practices used are still emerging. We are developing a better understanding of the nature and scale of the potential problem and effective interventions.

Harm: Online abuse of public figures **Box 14**

Threat:

In recent years we have seen a worrying rise in the amount of abuse, harassment and intimidation directed at those in public life. Much of this abuse happens on social media.

Impact:

- An international survey of female journalists found two thirds (64%) had experienced online abuse – death or rape threats, sexist comments, cyberstalking, account impersonation, and obscene messages.[46] Almost half (47%) did not report the abuse they had received, and two fifths (38%) admitted to self-censorship in the face of this abuse.[47]
- The Guardian's research into the 70 million comments left on its site over a ten year period highlighted that of the ten most abused writers, eight were women and two were black men. This is in spite of the fact that the majority of the regular opinion writers for The Guardian are white men. This was then compared to the ten writers who received the least abuse – who were all men.[48]

46 IFJ (2018). IFJ global survey shows massive impact of online abuse on women journalists. Available at: https://www.ifj.org/media-centre/news/detail/article/ifj-global-survey-shows-massive-impact-of-online-abuse-on-women-journalists.html
Note no similar data is available for male journalists.

47 Ibid.

48 The Guardian (2016). The dark side of Guardian comments. Available at: https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

There are too many stories of public figures closing their social media accounts following waves of abuse:

- In December 2017 the Committee for Standards in Public Life, which was commissioned by the Prime Minister, published its report on intimidation in public life.[49] The consultation sought views on a range of ideas including establishing a new offence of intimidation, and requiring imprints on electronic campaigning. The report included examples of the extent of intimidation of those in public life.
- "It is hard to explain how it makes you feel. It is anonymous people that you've never met, true, but it has a genuinely detrimental effect on your mental health. You are constantly thinking about these people and the hatred and bile they are directing towards you." – Rachel Maclean MP
- "I spoke on a number of occasions in the House of Commons in different committees about the rights of women. To which I suffered daily attacks on Twitter, on my email system or endless online articles written about how people wished to see me raped." – Jess Phillips MP
- The report also makes a number of recommendations for actions that social media companies should take in relation to intimidatory content, including implementing tools to enhance the ability of users to tackle online intimidation and supporting users who become victims of this behaviour.[50] These recommendations have helped to shape the indicative list of steps the regulator may want to include in codes of practice.
- The government's response to the Committee on Standards in Public Life's Review of Intimidation in Public Life was published in March 2018 and set out a number of actions for government based on the Committee's recommendations. As part of this work the government has undertaken a public consultation entitled Protecting the Debate: Intimidation, Influence and Information which closed in October 2018. The government's response will be published in due course.

This abuse is unacceptable – it goes beyond free speech and free debate, dissuades good people from going into public life, and corrodes the values on which our democracy rests.

The new regulatory framework will make clear companies' responsibility to address this harm.

Other online harms

1.26 There are other harms associated with the internet and online technology. For example, Ofcom and ICO's report on Internet Regulation highlighted users' concerns around privacy and hacking.[51] This White Paper is part of the government's wider programme of work to establish the right norms and rules for the internet.

49 Committee on Standards in Public Life (2017). Intimidation in Public Life. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/666927/6.3637_CO_v6_061217_Web3.1__2_.pdf

50 Government action to date is available here: https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-03-07/HCWS1389/

51 Ofcom and ICO (2018). Internet users' experience of harm online. Available at: https://www.ofcom.org.uk/research-and-data/Internet-and-on-demand-research/Internet-use-and-attitudes/Internet-users-experience-of-harm-online

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Responsible and ethical technology

1.27 The government takes both the protection of personal data and the right to privacy extremely seriously. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), alongside the increased powers for the ICO to gather evidence, inspect artificial intelligence (AI) and levy significant fines on those who break the law, update our data protection laws fit for the digital age.

1.28 The DPA also includes an important new provision requiring the Information Commissioner to produce an age-appropriate design code. This provision breaks new ground by addressing the approach to the design of online services likely to be used by children. It ensures platforms and service providers put child user interests at the centre of the design process, and protects them from risks that arise from the use of their personal data online, including the algorithms and profiling that serves them with personalised content.

1.29 However, the increased use of data and AI is giving rise to complex, fast-moving and far-reaching ethical and economic issues that cannot be addressed by data protection laws alone. Increasingly sophisticated algorithms can glean powerful insights, which can be deployed in ways that influence the decisions we make and the services we receive. It is essential that we understand, and respond to, barriers to the ethical deployment of AI.

1.30 That is why the government has set up the Centre for Data Ethics and Innovation. The Centre will provide independent, impartial and expert advice on the ethical and innovative deployment of data and AI. The Centre will publish its first strategy document in spring 2019, setting out further details on its key priorities.

1.31 The way that technology is designed, who it is designed by and the outcomes it is trying to achieve also influence how it impacts its users and wider society. There is an increasing amount of evidence that social media platforms and other digital services can impact people's habits, sleep patterns, productivity at work, attention spans and even voting preferences – see Box 15. We are looking carefully at how we can ensure that digital products and services are designed in a responsible way, with their users' well-being in mind. Chapter 8 of this paper looks specifically at how we are working with companies to include considerations around safety in the design of their products.

Emerging challenge: Designed addiction **Box 15**

Some online products have been designed to encourage continuous use. They include seemingly small but influential features, which incentivise people to keep using the app or platform for longer. One common example is the 'infinite scroll', in which information is loaded continuously as the user scrolls down the page, encouraging the user to keep scrolling.

- A recent report by 5Rights highlighted other elements of 'persuasive design', such as 'typing bubbles', quantifying friends, and notifications. Even 'likes' can be powerful tools for keeping users online.[52]

52 5Rights (2018). Disrupted Childhood: The Cost of Persuasive Design, 5Rights. Available at: https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- These techniques could exacerbate addictive behaviours. The number of people suffering from clinical addiction in this way has not been reliably quantified, but there are well-documented extreme cases of vulnerable individuals for whom addiction has got in the way of social lives, sleep, physical activity and other parts of a healthy, balanced lifestyle.
- There is also evidence that a wider range of people experience less extreme forms of compulsive or habitual behaviour online. Some experts would stress that this compulsive behaviour is not clinical addiction.

Future action:

- The government shares concerns around designed addiction and is determined to ensure that we have sufficient evidence on this risk, and the right expectations of companies to design their products in safe ways.
- In the future, we expect the regulator will continue to support research in this area to inform future action and, if necessary, set clear expectations for companies to prevent harm to their users.
- We also expect companies to be transparent about design practices which encourage extended engagement, and to engage with researchers to understand the impact of these practices on their users.
- DCMS is continuing to work with the Gambling Commission and the industry on player protections in the online sector. In May 2018, we published the response to the Consultation on Proposals for Changes to Gaming Machines and Social Responsibility Measures, which set out a clear plan to strengthen player protections.
- Since then, a number of changes have been made to make gambling fairer and safer, including tightening advertising rules and launching GAMSTOP, the online self-exclusion scheme. Additionally, from May, the Gambling Commission will bring in changes that mean that age and identity must be verified before consumers can deposit money and gamble, and will require age verification before customers can access free-to-play demo games.

Thriving digital markets

1.32 The digital sector makes a huge contribution to our economy at £130.5 billion gross value added in 2017, equivalent to 7% of the UK gross value added. The sector has seen strong growth with an increase of 33% since 2010, compared to 29% for the total UK economy.[53] As the digital economy has grown, powerful new companies have emerged, often with very dominant market positions. This has raised questions about the competitiveness of digital markets and what this means for consumers.

1.33 The government's Modernising Consumer Markets Green Paper sought views on how well equipped the UK's competition regime is to manage emerging challenges, including the growth of fast-moving digital markets. We continue to consider policy options across the range of measures proposed in the green paper and are conducting a review of

53 DCMS (2019). Sectors Estimates 2017 (provisional): Gross Value Added. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759707/DCMS_Sectors_Economic_Estimates_2017_provisional_GVA.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

digital markets, due in summer 2019. This will be informed by the work of the independent Digital Competition Expert Panel, led by Professor Jason Furman which published its recommendations for government on 13 March 2019.

1.34 Professor Furman and the panel found that the digital economy has brought significant benefits but does not have enough competition. They called for a new digital markets unit to set and enforce a code of conduct so the largest digital companies know what are acceptable rules for competition. This new unit would give people more control over their data by enabling people to switch between platforms more easily. They also recommended changes to merger rules, and updating existing rules to improve enforcement over anticompetitive conduct. The government will consider these proposals and respond later in the year.

1.35 Thriving digital markets also rely on the innovative, efficient and fair use of data. In June 2018, the Secretary of State for DCMS announced that we would develop a National Data Strategy to ensure the UK is a world-leading data economy – unlocking the power of data across government and the wider economy, while building public trust and confidence in its use.

Online advertising

1.36 Online advertising plays a crucial role in the digital economy, with many free digital services, such as search engines or social networks, funded by advertising revenues. The online advertising ecosystem is highly complex, with much of the advertising space online bought through automated processes, and the velocity with which adverts are created and displayed is far higher than offline. Online advertising encourages and rewards the collection of user data (the more data a service has on a user the more effectively it can target adverts at them) and the holding of people's attention (the longer they use a service the more adverts they see).

1.37 This combination of factors has given rise to a number of issues caused by or related to online advertising. Work is already underway to address some of these:

- A Home Office-led working group on CSEA and terrorist content linked to advertising met in March 2019, following an initial meeting in December 2018, comprising representatives from advertising trade bodies, agencies, brands, law enforcement and the IWF. The working group's activity to date comprises actions to help ensure advertising is not supporting this kind of illegal activity.
- As part of the government's Childhood Obesity Plan, DCMS and the Department of Health and Social Care launched a consultation on 18 March 2019 on introducing a 9pm watershed on TV advertising of products high in fat, salt or sugar, and similar protections for children viewing adverts online.
- The Competition and Markets Authority is considering further work on digital advertising, although this is dependent on the outcome of EU exit negotiations.
- In November 2018 the Advertising Standards Authority published its strategy More Impact Online, which aims to put the protection of consumers online at the heart of its work over the next five years, and makes commitments to explore, for example, the use of machine learning and AI to improve regulation.
- In 2018, the ICO conducted an investigation into data analytics and micro targeting of political advertising online. The report, 'Democracy Disrupted?', highlighted the risks of personal data being abused in digital campaigning and made a number

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

of recommendations to improve transparency and data protection compliance. The ICO has also commenced a broader examination of the use of personal data in adtech.[54]

1.38 As announced in the DCMS Secretary of State's immediate response to the Cairncross Review, DCMS will conduct a review of how online advertising is regulated in the UK.

54 ICO (2018). Democracy disrupted? Personal information and political influence. Available at: https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

2: The harms in scope

Summary

- This White Paper sets out government action to tackle online content or activity that harms individual users, particularly children, or threatens our way of life in the UK, either by undermining national security, or by reducing trust and undermining our shared rights, responsibilities and opportunities to foster integration. It sets out an initial list of content and behaviour which will be in scope, as well as a list of harms which will be excluded.
- There is currently a patchwork of regulation and voluntary initiatives aimed at addressing these problems, but these have not gone far or fast enough to keep UK users safe online.
- Many of our international partners are also developing new regulatory approaches to tackle online harms, but the UK will be the first to tackle online harms in a coherent, single regulatory framework that reflects our commitment to a free, open and secure internet.

Harmful content or activity in scope of the White Paper

2.1 Table 1 below shows the initial list of online harmful content or activity in scope of the White Paper, based on an assessment of their prevalence and impact on individuals and society.

2.2 This list is, by design, neither exhaustive nor fixed. A static list could prevent swift regulatory action to address new forms of online harm, new technologies, content and new online activities.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Table 1: Online harms in scope

Harms with a clear definition	Harms with a less clear definition	Underage exposure to legal content
• Child sexual exploitation and abuse. • Terrorist content and activity. • Organised immigration crime. • Modern slavery. • Extreme pornography. • Revenge pornography. • Harassment and cyberstalking. • Hate crime. • Encouraging or assisting suicide. • Incitement of violence. • Sale of illegal goods/ services, such as drugs and weapons (on the open internet). • Content illegally uploaded from prisons. • Sexting of indecent images by under 18s (creating, possessing, copying or distributing indecent or sexual images of children and young people under the age of 18).	• Cyberbullying and trolling. • Extremist content and activity. • Coercive behaviour. • Intimidation. • Disinformation. • Violent content. • Advocacy of self-harm. • Promotion of Female Genital Mutilation (FGM).	• Children accessing pornography. • Children accessing inappropriate material (including under 13s using social media and under 18s using dating apps; excessive screen time).

2.3 There is already an effective response to some categories of harmful content or activity online. These will be excluded from the scope of the new regulatory framework to avoid duplication of existing government activity.

2.4 The following harms will be excluded from scope:

- All harms to organisations, such as companies, as opposed to harms suffered by individuals. This excludes harms relating to most aspects of competition law, most cases of intellectual property violation, and the organisational response to many cases of fraudulent activity. The government is leading separate initiatives to tackle these issues. For example, the Joint Fraud Taskforce is leading an ambitious programme of work to tackle fraud, including online fraud, through partnership between banks, law enforcement and government.
- All harms suffered by individuals that result directly from a breach of the data protection legislation, including distress arising from intrusion, harm from unfair processing, and any financial losses. Box 16 explains how the UK's legal framework provides protection against online harms linked to data breaches.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- All harms suffered by individuals resulting directly from a breach of cyber security or hacking. These harms are addressed through the government's National Cyber Security Strategy.
- All harms suffered by individuals on the dark web rather than the open internet. These harms are addressed in the government's Serious and Organised Crime Strategy. A law enforcement response to criminality on the dark web is considered the most effective response to the threat. As set out in the strategy, the government continues to invest in specialist law enforcement skills and capability.

Stronger regulation of personal data online **Box 16**

The UK already enjoys high standards of data protection law, that were modernised in 2018 with the introduction of the GDPR and the Data Protection Act 2018. The government chose to go further than other countries, by providing stronger powers to apply to the investigation and enforcement of specific online threats.

Key protections for online harms involving personal data include:

- An obligation to provide clear and accessible privacy information, tailored for children when they are the users of online services.
- A legal obligation to accountability, making companies responsible for placing data protection at the centre of the design of online services in a way that mitigates the risk to users' information. This also includes a requirement to undertake data protection impact assessments, and have them approved by the ICO where high risks persist.
- A right to erasure of personal data online, with stronger provisions where data has been gathered from a child user.
- An age-appropriate design code, which gives the design standards we will expect providers of online services and apps used by children to meet when they process their data.
- A power to inspect algorithms in situ, to understand their use of personal data and whether this leads to bias or other detriment.
- A power to require information to be handed over to the ICO wherever it is held, including on cloud servers.

Shortcomings of the current regulatory landscape

2.5 Currently there is a range of UK regulations aimed at specific online harms or services in scope of the White Paper, but this creates a fragmented regulatory environment which is insufficient to meet the full breadth of the challenges we face. The current regulatory framework includes:

- GDPR and the Data Protection Act enforced by the ICO. This includes collection and use of personal data, including when online. The GDPR also has extraterritorial scope and can be enforced against companies outside the UK who offer services to UK users.[55]

55 The Information Commissioner's Office. Available at: https://ico.org.uk/

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- The Electoral Commission's oversight of the activity of political parties, and other campaigners, including activity on social media.[56]
- Forthcoming age verification requirements for online pornography.[57]
- The Equality and Human Rights Commission's oversight of the Equality Act 2010 and Freedom of Expression.[58]
- Ofcom's existing oversight of video-on-demand services.[59]
- The revised EU Audiovisual Media Services Directive, which will introduce new high-level requirements for video sharing platforms such as YouTube.[60]
- The Gambling Commission's licensing and regulation of online gambling.[61] DCMS has been working with the Commission to tighten advertising rules on gambling and launched GAMSTOP, the online self-exclusion scheme. Additional age-verification requirements are expected to come take effect in from May this year[62].
- The Competition and Markets Authority's (CMA) enforcement of consumer protection law online. See Box 17 for further details.

Consumer enforcement by the Competition and Markets Authority **Box 17**

Businesses risk breaching consumer protection law where their online behaviour misleads consumers or treats them unfairly. The CMA has undertaken a range of recent enforcement activity examining potentially unfair or misleading online behaviour, including:

- Online gambling – the CMA worked with the Gambling Commission to sanction unfair online 'bonus' promotions by major gambling firms. The CMA was concerned that players' money could effectively be trapped under the terms of these promotions, or that they could be caught out by unclear or imbalanced promotion rules. Changes were agreed with a number of firms, including William Hill and Ladbrokes.
- Online reviews and endorsements – the CMA has an ongoing programme of work to tackle fake or misleading online reviews and endorsements. Most recently, 16 celebrities, reality stars and social media influencers committed to always be clear

56 The Political Parties, Elections and Referendums Act 2000 (PPERA) provides the Electoral Commission with the powers and functions to regulate political finance in the UK. Electoral law is also enforced by the police, who lead on the Representation of the People Act offences. The Electoral Commission has powers to investigate breaches of the rules to funding and spending for election and referendum campaigns, which includes digital campaigning.

57 The Digital Economy Act 2017 provides for the regulation of providers of online commercial pornography to ensure that pornographic material is not normally accessible by those under 18, and that content which is deemed to be extreme pornographic material is not made available to any user. The BBFC is the designated regulator. These requirements will come into force shortly.

58 The Equality and Human Rights Commission. Equality Act 2010. Available at: https://www.equalityhumanrights.com/en/equality-act/equality-act-2010

59 The EU's Audiovisual Media Services Directive 2010 provides Ofcom with the power to regulate editorial content (programming) on UK 'video-on-demand' services – overseeing compliance on content requirements that cover protecting under 18s, preventing incitement to hate, and commercial references in programmes.

60 The EU's revised Audiovisual Media Services Directive (2018) will place requirements on 'video sharing platforms' to take 'appropriate measures' to protect minors from harmful content, protect the general public from illegal content and content that incites violence and/or hatred, and will introduce basic requirements around advertising. A regulator is still being selected, and these requirements are scheduled to come into force by September 2020.

61 The Gambling Act 2005 provides the Gambling Commission with powers to license and regulate all forms of gambling, including online gambling.

62 From May 2019, the Gambling Commission will bring in changes that mean that age and identity must be verified before consumers can deposit money and gamble, and will require age verification before customers can access free-to-play demo games.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

in their social media posts where they have been paid to post content online. The CMA is now examining the responsibility of social media platforms to ensure that paid-for content is always properly disclosed.

- Secondary tickets – as a result of action by the CMA, including court proceedings against Viagogo, consumers will always receive essential information before they purchase a ticket from online resale platforms, in particular if there is a risk that the consumer will not be able to get into the event or venue. The court order secured against Viagogo also requires that 'pressure selling' messages are removed from their website.
- Online hotel booking – the CMA recently agreed changes with companies in the Booking.com and Expedia corporate groups in relation to potentially misleading online practices. These include new requirements to be clear about the role that commission plays in the order of search results and that any claims about the limited availability of hotel rooms are accurate and do not risk misleading consumers.

2.6 Under the current liability regime, which is derived from the EU's e-Commerce Directive, platforms are protected from legal liability for any illegal content they 'host' (rather than create) until they have either actual knowledge of it or are aware of facts or circumstances from which it would have been apparent that it was unlawful, and have failed to act 'expeditiously' to remove or disable access to it. In other words, they are not liable for a piece of user-generated illegal content until they have received a notification of its existence, or if their technology has identified such content, and have subsequently failed to remove it from their services in good time.

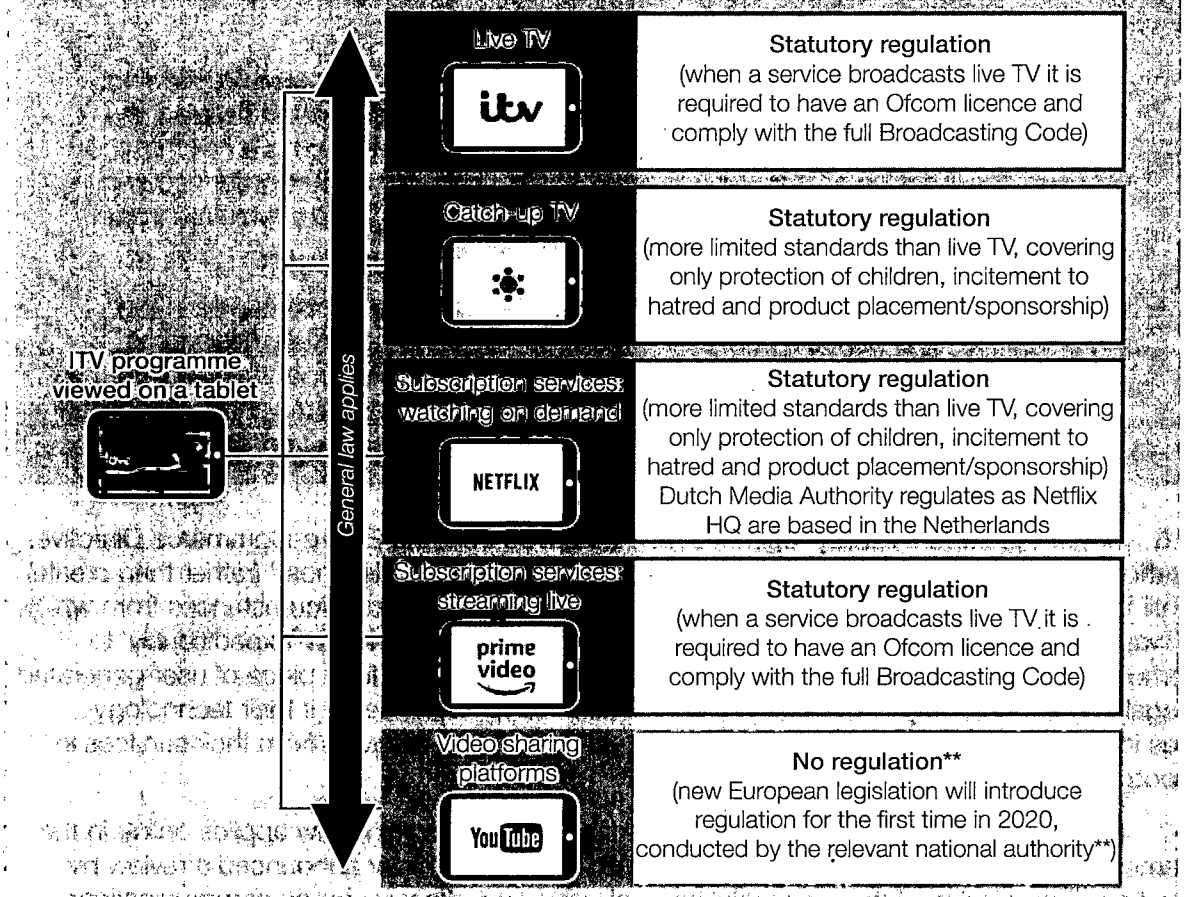
2.7 For illegal harms, it is also important to make sure that criminal law applies online in the same way as it applies offline. In February 2018 the Prime Minister announced a review by the Law Commission of the law in relation to abusive and offensive online communications, to highlight any gaps in the criminal law which cause problems in tackling this abuse. In its scoping report last year, the Law Commission concluded that behaviour is broadly criminalised to the same extent online as offline and recommended a clarification of existing communication offences. The government is now finalising the details of the second phase of the Law Commission work.

2.8 For legal harms, the same piece of content can be subject to different regulatory standards depending on the platform on which it appears. Ofcom's report Addressing Harmful Content Online sets out how the same programme would be regulated to differing degrees depending on whether it is broadcast on TV, viewed on-demand, or on an online video sharing platform (see Box 18). This means that there are significant gaps in consumer protection.[63]

63 Ofcom (2018). Addressing Harmful Online Content. Available at: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/online-policy-research/addressing-harmful-online-content

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Regulation of the same content on different services **Box 18**



Source: Addressing Harmful Content Online, Ofcom 2018.

Voluntary approaches

2.9 Beyond this range of regulatory requirements, the government's Internet Safety Strategy Green Paper, published in 2017, focused on a voluntary approach to countering harmful behaviour and content online. The green paper recognised that government alone cannot keep citizens safe from online harms, and sought to work in close partnership with industry to put in place specific technical solutions to make social media platforms safer.

2.10 Voluntary initiatives between government, industry and civil society are promising in some areas, and the leading companies have taken a number of steps to improve their platforms, for example as set out in Boxes 19-21. We are clear that the progress made on terrorism and CSEA through this voluntary cooperation with the industry must continue, alongside the development of a new regulatory framework.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Existing initiatives to tackle online harms: Global Internet Forum to Counter Terrorism **Box 19**

Following the Westminster terrorist attack in March 2017, the government convened a roundtable with major industry players, including Facebook, Twitter, Google and Microsoft to see what more could be done to tackle terrorist content online. This led to these companies setting up the Global Internet Forum to Counter Terrorism (GIFCT) in June 2017.

The GIFCT is leading the cross-industry response to reduce the availability of terrorist content on the internet so that there are no safe spaces for terrorists online. Key objectives for the Forum are to increase the use of automation and machine learning technology to detect and remove terrorist content – ultimately preventing terrorist content being made available to users in the first place – and supporting smaller, less well-resourced companies to tackle these threats on their own platforms.

The Forum has taken some positive steps since its establishment, but there is still much more to do. The government wants to see an ambitious and tangible plan for delivery. Our aims for the GIFCT in 2019 are for the Forum to:

- Expand its membership, securing a greater range and quantity of companies to sign up as members of the Forum.
- Devote greater efforts to targeted interventions with priority platforms, including through the development and sharing of automated technology.
- Put in place a clear programme of activity, providing metrics against which success can be measured.
- Provide greater visibility to drive this agenda forward, including companies having a clearer public voice on the issue.

Existing initiatives to tackle online harms: UK Council for Internet Safety **Box 20**

The UK Council for Internet Safety (UKCIS) is a new collaborative forum through which government, the tech community and civil society work together to ensure the UK is the safest place in the world to be online.

Expanding the scope of the former UK Council for Child Internet Safety (UKCCIS), UKCIS works to tackle online harms such as hate crime, extremism and violence against women and girls, in addition to maintaining a focus on the needs of children.

Priority areas of delivery for UKCIS over the next year include:

- Producing a landscape review of research around adult online harms, and regular concise summaries of emerging research.
- Updated guidance to schools on sexting, and evaluation of online safety provision, and for Initial Teacher Training providers to help them upskill new teachers in online safety.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Promoting the Connected World framework, which describes the digital knowledge and skills that children should have the opportunity to develop at different stages of their lives.
- A digital resilience framework and toolkit to help families, educators, policymakers, frontline service workers and the industry better support users online, across a wide range of harms.

Existing initiatives to tackle online harms: WePROTECT Global Alliance **Box 21**

The WePROTECT Global Alliance (WPGA) was established in recognition that CSEA is a global crime requiring a global response.

The UK government played a key role in establishing WPGA and is its sole financial donor. WPGA aims to protect more children, apprehend more perpetrators of abuse and make the internet free from child sexual exploitation. Eighty-five countries are members of WPGA, along with 20 global technology companies and 25 leading non-governmental organisations.

The success of the UK government funded WPGA is that it has brought together government, law enforcement, industry and civil society to take a stand against online child sexual exploitation.

2.11 In the Government Response to the Internet Safety Strategy Green Paper consultation, we noted that only a relatively small group of the larger companies are engaged with the government's work on online safety, even though online harms can and do occur across many websites. There is also a wide variation in the extent, efficacy and pace of actions by companies to tackle online harms. Some companies rely on user moderation to oversee reported violations of their terms and conditions, such as Reddit; others employ teams of moderators or deploy technology to monitor content, such as Facebook.

2.12 Many companies claim to hold a strong track record on online safety but there is limited transparency about how they implement or enforce their policies, and there is a persistent mismatch with users' experiences – 70% of Britons believe that social media companies do not do enough to prevent illegal or unethical behaviours on their platforms.[64] 60% of respondents to our Internet Safety Strategy Green Paper consultation had witnessed inappropriate or harmful behaviour online; only 41% thought their reported concerns were taken seriously by social media companies.[65]

2.13 At present many online companies rely on using their terms and conditions as the basis by which to judge complaints. In practice however, companies' terms and conditions are often difficult for users to understand, and safety policies are not consistent across different

64 Edelman (2018). Edelman Trust Barometer – UK Findings. Available at: https://www.edelman.co.uk/magazine/posts/edelman-trust-barometer-2018/

65 HM Government (2018). Government Response to the Internet Safety Strategy Green Paper. May 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

platforms, with take-down times, description of harms and reporting processes varying. A series of investigations have highlighted the risk of serious shortcomings in the training, working conditions and support provided for content moderators.[66]

2.14 There is no mechanism to hold companies to account when they fail to tackle breaches. There is no formal, wide-reaching industry forum to improve coordination on terms and conditions. The absence of clear standards for what companies should do to tackle harms on their services makes it difficult for users to understand or uphold their rights.

2.15 The government believes that voluntary efforts have not led to adequate or consistent steps to protect British citizens online. As highlighted above, users' own experiences confirm a sense of vulnerability online.

An international approach

2.16 The threat posed by harmful and illegal content and activity online is a global one, and many of our international partners are also developing new regulatory approaches to tackle online harms. Box 22 sets out what some other countries are doing in this area.

International approaches to countering online harms **Box 22**

Germany adopted its Network Enforcement Act (NetzDG) in 2017. This law requires online platforms with more than two million registered users in Germany to remove 'manifestly unlawful' content, which contravenes specific elements of the German criminal code, such as holocaust denial and hate speech, within 24 hours of receiving a notification or complaint, and to remove all other 'unlawful' content within seven days of notification. Non-compliance risks a fine of up to €50 million. This law also seeks to increase platform responsibility through imposing greater transparency and significant reporting obligations.

Australia established an eSafety Commissioner through its Enhancing Online Safety for Children Act in 2015. The eSafety Commissioner is responsible for promoting online safety for all Australians. As well as offering a complaints service for young people who experience serious cyber bullying, its remit includes identifying and removing illegal online content and tackling image-based abuse.

The European Commission, led by DG JUST, published in September 2018 a proposal on preventing the dissemination of terrorist content online – Member States agreed a Council version of the text in December 2018. The aim of the proposal is to ensure a consistent approach across industry to the removal of online terrorist content by Hosting Service Providers, for example social media platforms and video sharing sites. There are similarities in the approach taken to the framework proposed in this White Paper – as currently drafted it looks to take a proportionate approach to setting requirements, introduce duties of care on companies, and implementing a transparency framework.

Over 2018, the EU Commission, led by DG CNECT, also published its Action Plan against Disinformation. The Commission collaborated with companies including Facebook, Google and Twitter to produce a code of practice against disinformation. This resulted in commitments to improve the transparency of political advertising, prevent the misuse

66 The Verge (2019). The Trauma Floor. Available at: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

of automated bots and to invest in tools to amplify diverse perspectives. The UK government has previously indicated its support for the measures and will continue to collaborate internationally on this issue.

2.17 The government is working closely with international partners as we develop our own approach that reflects our shared values and commitment to a free, open and secure internet. The approach proposed in this White Paper is the first attempt globally to tackle this range of online harms in a coherent, single regulatory framework. We will continue to share experiences and seek to work with international partners. Further details are set out in Chapter 6.

Existing initiatives to tackle online harms: Project Arachnid **Box 23**

The government has invested £600,000 into Project Arachnid, a groundbreaking project that trawls the web to identify web pages with suspected child sexual abuse material. The technology can be deployed across websites, forums, chat services and newsgroups to instantaneously detect illegal content, before sending a take-down notice to service providers so they can quickly protect children from further exploitation.

Project Arachnid is the product of a partnership with the Canadian Centre for Child Protection and the US National Center for Missing and Exploited Children, demonstrating the UK's determination to work with international partners to tackle harmful activity online. To date, Arachnid has trawled 1.5 billion webpages, detected 7.5 million suspected images of child sexual abuse and issued more than 1 million take-down notices for the removal of child abuse material on the open web.[67]

67 Live dashboard data, data taken on 21 March 2019.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

PART 2: Regulatory model

3. A new regulatory framework

Summary

- The government will establish a new statutory duty of care to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services. Compliance with this duty of care will be overseen and enforced by an independent regulator.
- Companies must fulfil their new legal duties. The regulator will set out how to do this in codes of practice. If companies want to fulfil these duties in a manner not set out in the codes, they will have to explain and justify to the regulator how their alternative approach will effectively deliver the same or greater level of impact.
- Regarding the threat to national security or the physical safety of children, the government will have the power to direct the regulator in relation to codes of practice relating to terrorist activity or CSEA online, and these codes must be signed off by the Home Secretary.
- For all codes of practice relating to illegal harms, including incitement of violence and the sale of illegal goods and weapons, there will be a clear expectation that the regulator will work with law enforcement and other relevant government agencies to ensure the codes adequately keep pace with the threat.
- Developing a culture of transparency, trust and accountability will be a critical element of the new regulatory framework. The regulator will have the power to require annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms and what measures they are taking to address this. These reports will be published online by the regulator, so that users and parents can make informed decisions about online use. The regulator will also have powers to require additional information, including about the operation of algorithms.
- The regulator will encourage and oversee the fulfilment of companies' commitments to improve the ability of independent researchers to access their data, subject to appropriate safeguards.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- As part of the new duty of care, we will expect companies, where appropriate, to have an effective and easy-to-access user complaints function. The regulator will require companies to respond to user complaints within an appropriate timeframe and to take action consistent with the expectations set out in the regulatory framework.
- But we also recognise the importance of an independent review mechanism to ensure that users have confidence that their concerns are being treated fairly. We are consulting on allowing designated bodies to make 'super complaints' to defend the needs of users.
- Ahead of the implementation of the new regulatory framework, we will encourage companies to take early action to address online harms. To assist this, the White Paper sets out high-level expectations of companies, including some specific expectations in relation to certain harms. We expect the regulator to reflect these in future codes of practice.
- Where there is a threat to national security or the physical safety of children, such as CSEA and terrorism, we will expect companies to go much further and demonstrate the steps taken to combat the dissemination of associated content and illegal behaviours. We will publish interim codes of practice providing guidance about tackling terrorist activity and online CSEA later this year.

3.1 The government will establish a new statutory duty of care on relevant companies to take reasonable steps to keep their users safe and tackle illegal and harmful activity on their services.

3.2 The fulfilment of this duty will be overseen and enforced by an independent regulator.

3.3 This statutory duty of care will require companies to take reasonable steps to keep users safe, and prevent other persons coming to harm as a direct consequence of activity on their services. This broader application of the duty, beyond simply users of a particular service, recognises that in some cases the victims of harmful activity – victims of the sharing of non-consensual images, for example – may not themselves be users of the service where the harmful activity took place. This duty will apply to all of the harms included in the scope of the White Paper, as set out below.

3.4 A key element of the regulator's approach will be the principle of proportionality. Companies will be required to take action proportionate to the severity and scale of the harm in question. The regulator will be required to assess the action of companies according to their size and resources, and the age of their users.

3.5 The regulatory approach will impose more specific and stringent requirements for those harms which are clearly illegal, than for those harms which may be legal but harmful, depending on the context.

3.6 Companies must fulfil their new legal duties. The regulator will set out how to do this in codes of practice. The codes will outline the systems, procedures, technologies and investment, including in staffing, training and support of human moderators, that companies need to adopt to help demonstrate that they have fulfilled their duty of care to their users.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Companies will still need to be compliant with the overarching duty of care even where a specific code does not exist, for example assessing and responding to the risk associated with emerging harms or technology.

3.7 There will be a strong expectation that companies follow the guidance set out in these codes. If they choose not to do so, companies will have to explain and justify to the regulator how their alternative approach will effectively deliver the same or greater level of impact. This approach is familiar to companies, for example the UK Corporate Governance Code[68] and the ICO's code of practice on data sharing. Though these codes will be developed with the companies and other stakeholders in an open and transparent way, the regulator will ultimately decide on their content.

3.8 The regulator will assess whether companies have fulfilled their duty of care, including by reference to relevant codes of practice, and compliance with the company's own relevant terms and conditions. Failure to meet these obligations may result in enforcement action by the regulator. Further details on enforcement are in Chapter 6.

3.9 The regulator will also expect companies to make clear how they are fulfilling their statutory duty of care. Relevant terms and conditions will be required to be sufficiently clear and accessible, including to children and other vulnerable users. The regulator will assess how effectively these terms are enforced as part of any regulatory action.

Terrorism and CSEA online

3.10 Companies will be required to take particularly robust action to tackle terrorist use of the internet and online CSEA. The government will have the power to issue directions to the regulator regarding the content of the codes of practice for these harms, and will also approve the draft codes before they are brought into effect. Similarly, the regulator will not normally agree to companies adopting proposals which diverge from these two codes of practice, and will require a high burden of proof that alternative proposals will be effective.

3.11 Between the publication of this White Paper and the establishment of a regulator, the government will work with law enforcement and other relevant bodies to produce interim codes of practice for online terrorist content and CSEA. These codes will be published later this year.

General monitoring

3.12 The regulator will not compel companies to undertake general monitoring of all communications on their online services, as this would be a disproportionate burden on companies and would raise concerns about user privacy. The government believes that there is however, a strong case for mandating specific monitoring that targets where there is a threat to national security or the physical safety of children, such as CSEA and terrorism.

Transparency, trust and accountability

3.13 Developing a culture of transparency, trust and accountability, and consistent standards of transparency, will be a critical element of the new regulatory framework.

68 Financial Reporting Council (2018). UK Corporate Governance Code. Available at: https://www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3.14 In May 2018, the Government Response to the Internet Safety Strategy Green Paper consultation set out the role transparency and reporting must play in building our understanding of the extent of online harms and how effectively companies are tackling breaches in their terms and conditions.

3.15 Alongside this response, we published a draft transparency reporting template and began a series of engagements with industry. This process, which has included discussion with over 20 companies, has provided some helpful insights into current industry action. It is encouraging that more companies have since started publishing their own global transparency reports. We will publish the government's first annual transparency report later this year.

3.16 At the same time, we indicated that transparency reporting was one of the potential areas for new legislation. Greater transparency will ensure:

- The regulator can gain an understanding of the level of harms on online platforms and the mitigating action being taken by companies. This will inform its regulatory priorities and determine the effectiveness of, and compliance with, different regulatory measures.
- Users can gain a greater understanding and awareness of whether and to what extent companies are taking positive steps to keep their users safe, and the processes different companies have in place to prevent harms.
- Companies take responsibility for the impacts of their platforms and products on their users. It will incentivise accountability within the industry.

3.17 To inform its reports and to guide its regulatory action, the regulator will have the power to require annual reports from companies covering the following areas:

- Evidence of effective enforcement of the company's own relevant terms and conditions, which should reflect guidance issued by the regulator in its codes of practice.
- Processes that the company has in place for reporting illegal and harmful content and behaviour, the number of reports received and how many of those reports led to action.
- Proactive use of technological tools, where appropriate, to identify, flag, block or remove illegal or harmful content.
- Measures and safeguards in place to uphold and protect fundamental rights, ensuring decisions to remove content, block and/or delete accounts are well-founded, especially when automated tools are used and that users have an effective route of appeal.
- Where relevant, evidence of cooperation with UK law enforcement and other relevant government agencies, regulatory bodies and public agencies.
- Details of investment to support user education and awareness of online harms, including through collaboration with civil society, small and medium sized enterprises (SMEs) and other companies.

3.18 The regulator will produce and publish an annual transparency report outlining key data on companies' performance against their duty of care and the prevalence of harms on different platforms. It will also publish companies' transparency reports on its website, ensuring these are easily accessible to the public so that users and parents can make

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

informed decisions about online use. Where the regulator has required companies to produce transparency reports, it will be mandatory to provide them; failure to do so will result in enforcement action (as set out in Chapter 6).

3.19 The regulator will use insight from users, civil society, government, law enforcement and other relevant government agencies, and other regulators to inform its understanding of the prevalence and impact of online harms, and the effectiveness of companies' responses.

3.20 As well as the power to require annual reports from companies, the regulator will have the power to require additional information from them to inform its oversight or enforcement activity, and to establish requirements to disclose information. It may also undertake thematic reviews of areas of concern, for example a review into the treatment of self-harm or suicide related content. The regulator will have the power to require companies to share research that they hold or have commissioned that shows that their activities may cause harm.

3.21 The regulator will build on government engagement with companies to understand how best to establish comparable data-points and reporting between platforms.

3.22 As part of a movement towards greater transparency, companies should also work in conjunction with the regulator to build a shared understanding of the mechanics of their associated platforms or services. Where necessary, to establish that companies are adequately fulfilling the duty of care, the regulator will have the power to request explanations about the way algorithms operate. The regulator may, for example, require companies to demonstrate how algorithms select content for children, and to provide the means for testing the operation of these algorithms.

3.23 In determining where such explanations will be appropriate and what form they should take, the regulator will work closely with the Centre for Data Ethics and Innovation, the expert body that has been set up to advise government on the regulation of data, including algorithmic tools. Appropriate safeguards will be needed to ensure commercial confidentiality, although the regulator is unlikely to require direct access to companies' proprietary codes if necessary explanations have been provided.

3.24 Several of the largest companies have promised access for independent researchers to anonymised information, in line with data protection requirements. This is a positive step, although it is as yet unclear whether these promises have been fulfilled. The government welcomes these steps, and believes that this level of transparency to researchers is a necessary part of developing the increased understanding of online harms. We will task the regulator with encouraging this approach, and ensuring companies make relevant information available.

3.25 We will expect the regulator to foster a culture of cooperation between companies and to encourage companies, especially the larger ones, to share information about online harms. Users perpetrating harm often move between platforms, especially to behave illegally and disseminate illegal content. A greater level of cooperation between platforms by sharing observations and best practices to prevent harms spreading from one provider to another will be essential.

Consultation questions

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

User redress

3.26 Many companies claim a strong track record on online safety, but responses to our Internet Safety Strategy Green Paper showed that this is at odds with users' experiences. To fulfil the new duty of care, we will expect companies, where appropriate, to have an effective and easy-to-access complaints function, allowing users to raise either concerns about specific pieces of harmful content or activity, or wider concerns that the company has breached its duty of care. Users should receive timely, clear and transparent responses to their complaints, and there must be an internal appeals function. The regulator will have oversight of these processes, including through transparency information about the volume and outcome of complaints, and the power to require improvements where necessary. Box 24 explains users' rights under the proposed requirements.

3.27 In addition to the internal appeals processes, we recognise that independent review or resolution mechanisms may be appropriate in some circumstances. This would increase the accountability of companies and help rebuild users' trust. We are consulting on the following option:

- Whether a provision should be made in legislation for designated bodies to bring 'super complaints' to the regulator for consideration, in specific and clearly evidenced circumstances. This could be an important safeguard in the user redress process and we are also consulting on when such complaints would be appropriate and most effective, and on the bodies or groups that may be empowered to bring them.

3.28 We would also welcome views during the consultation process on additional options for redress.

Consultation questions

Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

> Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

3.29 Under current arrangements, individuals can, in principle, obtain remedies in court against companies where they are negligent or breach their contract with the individual but such legal actions can face difficulties. For example, difficulties in establishing the company's duty of care to the person bringing the claim, showing a causal link between their activities and harm caused, or obtaining factual evidence. Our regulatory model will provide evidence and set standards which may increase the effectiveness of individuals' existing legal remedies.

3.30 The regulator's primary role in the user redress process will be to oversee the requirement on relevant companies to have appropriate and effective internal complaints processes, including consideration of whether there should be an appeals function in certain circumstances. The regulator would also determine any 'super complaints' process and designate bodies. We do not envisage a role for the regulator itself in determining disputes between individuals and companies, but where users raise concerns with the regulator, it will be able to use this information as part of its consideration of whether there may be systemic failings which justify enforcement action. We will also require the regulator to take the interests of users into consideration.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Regulation in practice: User redress: how the regulatory framework will work for individuals **Box 24**

At the moment, individuals can raise complaints and concerns about harmful online activity with companies, but processes vary and provision is patchy across the industry. Some companies do not have effective means to address user concerns, and it is not always clear what response, if any, a user will receive. Only two in five respondents to the government's consultation on the Internet Safety Strategy felt their concerns were taken seriously by social media companies. The regulatory framework proposed in this White Paper will give individuals new avenues to pursue complaints.

1. Right to an internal complaints procedure that meets standards set out by the regulator. Where appropriate, companies covered by the regulator will be required to have an effective complaints process, and the regulator will set minimum standards for these processes. This means that users will know how they can raise a complaint, how long it will take a company to investigate, and what response they can expect (including appeal rights).
2. Right of redress through an independent process. If the company is unable or unwilling to resolve a complaint, or the user is not satisfied with the response, it may be appropriate for users to be able to seek redress through an independent process. We are seeking views on how this could work in practice, including whether the regulator should run a 'super complaints' scheme through which designated organisations could raise issues with the regulator on behalf of users.
3. The ability to alert the regulator to an alleged breach of a company's duty of care. While the regulator would not normally adjudicate on individual complaints about companies, users will be able to report concerns to the regulator. This will be an important part of the regulator's horizon scanning to identify where companies might not be fulfilling their duty of care to their users.
4. The scope to use the regulator's findings in any claim against a company in the courts on grounds of negligence or breach of contract. And, if the regulator has found a breach of the statutory duty of care, that decision and the evidence that has led to it will be available to the individual to use in any private legal action.

Role of Parliament

3.31 It will be important to ensure that Parliament is able to scrutinise the regulator's work. Mechanisms for achieving this will depend in part on whether the regulator is a new or existing body but are likely to include, for example, a duty on the regulator to lay its annual report and audited accounts before Parliament. The regulator will also have a general responsibility to provide Parliament with information about its work, as requested.

3.32 In addition, we will consider what role Parliament should have in relation to the regulator's codes of practice. Parliament's role in relation to codes of practice and guidance issued by other regulators varies across different regulatory regimes, ranging from formal approval to no specific role. We will consider options for the role of Parliament as we develop these proposals in more detail.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Consultation questions

Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

4: Companies in scope of the regulatory framework

Summary

- The regulatory framework will apply to companies that provide services or tools that allow, enable or facilitate users to share or discover user-generated content, or interact with each other online.
- These services are offered by a wide range of companies, including start-ups and SMEs, and other organisations such as charities.
- The application of the regulatory requirements and the duty of care model will reflect the diversity of organisations in scope and ensure a risk-based and proportionate approach. We will minimise excessive burdens, particularly on small businesses and civil society organisations.
- Reflecting the importance of privacy, any requirements to scan or monitor content for tightly defined categories of illegal content will not apply to private channels. We are consulting on definitions of private communications, and what measures should apply to these services.

4.1 Harmful content and behaviour originates from and migrates across a wide range of online platforms or services, and these cannot readily be categorised by reference to a single business model or sector. Focusing on the services provided by companies, rather than their business model or sector, limits the risk that online harms simply move and proliferate outside of the ambit of the new regulatory framework. We propose that the regulatory framework should apply to companies that allow users to share or discover user-generated content, or interact with each other online.

4.2 There are two main types of online activity that can give rise to the online harms in scope or compound their effects:

- Hosting, sharing and discovery of user-generated content (e.g. a post on a public forum or the sharing of a video).
- Facilitation of public and private online interaction between service users (e.g. instant messaging or comments on posts).

4.3 A wide variety of organisations provide these services to users. This will mean that companies of all sizes will be in scope of the regulatory framework. The scope will include companies from a range of sectors, including social media companies, public discussion forums, retailers that allow users to review products online, along with non-profit organisations, file sharing sites and cloud hosting providers.

4.4 This comprehensive approach is important for the efficacy of the new regulatory framework.

4.5 We also recognise the importance of minimising undue burdens on organisations in scope and of avoiding uncertainty about how regulation will apply. To ensure a proportionate approach and avoid being overly burdensome, the application of the regulatory requirements and the duty of care model will reflect the diversity of organisations in scope, their capacities, and what is technically possible in terms of proactive measures, including for those providing ancillary services such as caching (the process of temporarily storing data in either a

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

software or hardware 'cache'). While we will minimise excessive burdens according to the size and resources of organisations, all companies will be required to take reasonable and proportionate action to tackle harms on their services. The regulator will ensure that there is clarity about what the regulatory regime means in practice for different company's, and will not impose new requirements where there is no evidence of harm. A range of proposed initiatives to counter regulatory burdens are set out in Chapter 6.

Regulatory approach to private communications

4.6 Defining 'private' and 'public' in the online space is complex from a technical and legal standpoint. For example, there is an obvious difference between one-to-one messaging, and a WhatsApp group of several hundred users. However, users should be protected from harmful content or behaviour wherever it occurs online, and criminals should not be able to exploit the online space to conduct illegal activity. The development of harmful activity online frequently involves a combination of activity taking place on both public and private communication channels. For example, terrorist propaganda is often disseminated over public channels, with activities such as the preparation of terrorist attacks occurring largely on private channels. Such private channels are also widely used to store and share images of CSEA, or to groom young children, with public channels frequently being where initial contact with a child takes place (see Box 25).

4.7 Reflecting the importance of privacy, the framework will also ensure a differentiated approach for private communication, meaning any requirements to scan or monitor content for tightly defined categories of illegal content will not apply to private channels.

4.8 We are consulting on appropriate definitions and what regulatory requirements can and should apply to private communication services alongside this White Paper.

Harm: Child sexual exploitation and abuse – how online grooming moves across different platforms **Box 25**

Evidence shows how grooming activity often migrates across platforms, luring children into less public spaces online:

- Initial contact with a child is often made after they are identified as a potential victim by a groomer on public social media platforms.
- Offenders may target children based on vulnerabilities such as mental health, or by exploiting publicly available information from their social media profiles.
- The grooming process can be extensive; building rapport and manipulating the victim – but it can also move almost immediately into sexual advances.
- This can involve the groomer then sending the child a message, using the same platform's private messaging service or another private or encrypted messaging service, seeking to extort indecent imagery and continue their abuse.

Consultation questions

Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

Question 6: In developing a definition for private communications, what criteria should be considered?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?

Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

PART 3: Regulation in practice

5: A regulator for online safety

Summary

- An independent regulator will implement, oversee and enforce the new regulatory framework. It will have sufficient resources and the right expertise and capability to perform its role effectively.
- The regulator will also have broader responsibilities to promote education and awareness-raising about online safety, and to promote the development and adoption of safety technologies to tackle online harms.
- The regulator will take a risk-based approach, prioritising action to tackle activity or content where there is the greatest evidence or threat of harm, or where children or other vulnerable users are at risk.
- To support this, the regulator will undertake and commission research to improve the evidence base, working closely with UK Research and Innovation (UKRI) and other partners.
- The regulator will take a proportionate approach, expecting companies to do what is reasonable, depending on the nature of the harm and the resources and technology available to them.
- The regulator will have a legal duty to pay due regard to innovation, and to protect users' rights online, being particularly mindful to not infringe privacy and freedom of expression.
- The government is consulting on whether the regulator should be a new or existing body. The regulator will be funded by the industry in the medium term, and the government is exploring options such as fees, charges or an industry levy to put it on a sustainable footing.

The functions of the regulator

5.1 The regulatory framework will be implemented, overseen and enforced by an independent regulator. This regulator will be equipped with the powers, resources and expertise it needs to effectively carry out its role.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

5.2 The regulator's functions will include:

- Setting out what companies need to do to fulfil the duty of care, including through codes of practice.
- Establishing a transparency, trust and accountability framework, backed by information-gathering powers, to assess companies' compliance with the duty of care and their own relevant terms and conditions.
- Providing support to start-ups and SMEs to help them fulfil their legal obligations in a proportionate and effective manner.
- Overseeing the implementation of user redress mechanisms.
- Taking prompt and effective enforcement action in the event of non-compliance (as set out in Chapter 6).
- Promoting education and awareness-raising about online safety to empower users to stay safe online.
- Promoting the development and adoption of safety technologies to tackle online harms.
- Undertaking and commissioning research to improve our understanding of online harms and their impacts on individuals and society.

A risk-based approach

5.3 The government will require the regulator to adopt a risk-based approach, prioritising regulatory action to tackle harms that have the greatest impact on individuals or wider society. This will shape the development of codes of practice, monitoring and review of online harms, the regulator's work with industry to develop technological solutions, and enforcement action.

5.4 The regulator will also focus on companies where there is the greatest risk of harm, based on factors such as the type of service – for example, services that enable adult users to contact children, services that have large user bases, and services that target or are popular with vulnerable groups of users. It will also use evidence of the actual incidence of harms on different services and the safety track record of different companies to prioritise its resources. The regulator will use its powers to conduct thematic reviews, undertake targeted horizon scanning and investigate specific issues to develop its understanding of the risk landscape.

5.5 This risk-based approach will mean that the regulator's initial focus in the first phase will be on those companies which pose the biggest and most obvious risk of harm to users, either because of the scale of the service's size or because of known issues with serious harms. We expect the regulator to take a proactive approach to assessing compliance in these cases, whereas their approach to the full range of companies in scope would be focused on providing advice and guidance and taking reactive action in response to concerns. This is consistent with the approach in a number of other regulatory regimes, including health and safety and financial services.

5.6 The duty of care approach will also mean companies must improve their understanding of the risks associated with their services and take effective and proportionate steps to mitigate these risks. These steps should be in keeping with the codes of practice set down by the regulator. When assessing compliance, the regulator will need to consider whether the harm was foreseeable, and therefore what is reasonable to expect a company to have done. In the event of a new risk emerging, the company should notify the regulator in order to discuss the best approach to mitigation and to share learning across companies.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

A proportionate approach

5.7 The regulator will take account of the capacity of companies to meet regulatory requirements, including the reach of their platforms in terms of user-base and the severity of the harms. This proportionate approach will also be enshrined in the legislation by making clear that companies must do what is 'reasonably practicable' – a test that has underpinned the success of health and safety legislation. However, all companies within scope will be required to take reasonable and proportionate action to tackle harms on their services, and the regulator will set clear expectations of what companies should do to tackle illegal activity and to keep children safe online.

5.8 We expect the regulator to comply with principles of regulatory best practice, which means that its activities will be sensitive to impacts on competition and small and micro-businesses in particular (see Box 26).

5.9 The regulator will also be required to support less well-resourced companies, as part of its work to develop tools to build capacity amongst companies and users. For example, we expect the regulator to work with the industry to encourage the development of technologies that aid compliance, and to facilitate cross-sector collaboration and sharing of expertise. These technologies could be made available to start-up or small companies. This is part of a wider advisory role for the regulator through which it will, for example, provide industry with technical information on best practice content moderation processes, or provide toolkits that explain common patterns of behaviour by cyberstalkers.

5.10 Through the consultation process alongside this White Paper, we intend to work with industry, civil society and the public to look at ways in which we can minimise any excessive burdens and provide additional certainty to businesses, and explore what more the regulator could do to make compliance straightforward and practicable for all businesses.

Regulation in practice: Better regulation principles and the new regulatory framework **Box 26**

We need all platforms to take reasonable steps to keep their users safe. Harm can occur on small platforms as well as big ones. There is nowhere on the internet where it is acceptable to host child sexual abuse material or terrorist material.

Regulation can impose a disproportionate burden on smaller companies. Badly designed regulation can stifle innovation by giving an advantage to large companies that can handle compliance more easily. We are determined that this regulatory framework should provide strong protection for our citizens while avoiding placing an impossible burden on smaller companies.

We will take five key steps to achieve this:

1. A proportionate approach. The regulator will take account of the capacity of companies to meet regulatory requirements, including their size and the reach of their platforms in terms of user-base, as well as the risk and prevalence of harms on their service.
2. A duty of innovation. The regulator will have a legal duty to pay due regard to innovation. This will include implementing the framework in a way that does not impose impossible demands on new and challenger companies. This will also ensure that start-ups and those developing innovative new products can work with the regulator, for example through regulatory sandboxes.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3. Making compliance straightforward. The regulator will be tasked with helping start-ups and SMEs fulfil their obligations. We will learn from best practice in other sectors, such as the support provided to companies by the Health and Safety Executive or the ICO.
4. Using technology. Government will work with the regulator to promote effective technological compliance solutions that can be made available to start-ups and small businesses.
5. Minimising compliance costs. We will explore options to streamline compliance, including creating machine executable regulation and facilitating easy, secure data sharing.

A legal obligation to support innovation

5.11 The regulator will have a legal obligation to pay due regard to innovation. A similar obligation was placed on the ICO under the Data Protection Act 2018. This has allowed the regulator to fully implement a robust data protection regime in a pro-innovation way. The ICO currently has plans to establish an initiative that will proactively support organisations to develop innovative products and services that make use of personal data and benefit the public. The ICO will provide this support whether these innovations are at design, proof of concept and testing stages, or as further ongoing development of existing innovative products/services. This is distinct from the legal requirement of data protection by design. We would expect the regulator to explore similar approaches to supporting and encouraging innovation in this space, subject to minimum expectations of user safety. This obligation will encourage the regulator to take a flexible, proportionate and risk-based approach when setting and enforcing expectations and responsibilities for companies.

Protecting users' rights online

5.12 The regulator will also have an obligation to protect users' rights online, particularly rights to privacy and freedom of expression. It will ensure that the new regulatory requirements do not lead to a disproportionately risk averse response from companies that unduly limits freedom of expression, including by limiting participation in public debate. Its regulatory action will be required to be fair, reasonable and transparent.

Empirical approach

5.13 The new regulator will take an evidence-based approach to regulatory activity. It will need to understand the potential impact of technological developments on the companies it regulates, as well as users' experiences of harm. To support this, we expect that it will run a regular programme of user consultation, in-depth research projects, and horizon scanning activity. It will work with companies to ensure that academics have access to company data to undertake research, subject to suitable safeguards. This dynamic approach to evidence gathering will help the regulator to assess the changing nature of harms and the risks associated with them, and of the places and manner in which they manifest online.

5.14 The regulator will work closely with UKRI to ensure support for targeted research into online harms, and to develop the collective understanding of online harms and the evidence base, building on the work of the UKCIS Evidence Group. This will include working with relevant aspects of UKRI's Digital Economy Theme – a partnership between the Engineering and Physical Sciences Research Council (EPSRC), the Arts and Humanities Research Council (AHRC), the Economic and Social Research Council (ESRC) and Innovate UK.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The regulatory body

5.15 An independent regulator could be set up, either by creating a new body, or by altering the remit and functions of an existing organisation. The usual government approval processes would apply to the establishment of a new central government regulatory body. The government is considering:

- A new regulator. Setting up a dedicated new regulator would provide a clear and coherent remit to focus on online safety and provide new leadership of online safety to industry and the public. A new body would, however, be more costly to set up and take longer to become operational and risks further complicating the regulatory landscape.
- An existing regulator. Tasking an existing regulator to assume responsibility for online safety would mean that the new regime would start with regulatory credibility and make the best use of existing experience and expertise. We would assess existing regulators' suitability based on their current responsibilities, the type of regulation they are already responsible for, their track record of working successfully within complex sectors, and their capacity to take on new responsibilities for online safety, including compatibility with their current legal status and operating model.

5.16 If we were to establish a new, dedicated regulator over the long term, we would need to consider options for the interim period, given the time it would take to set up a new body. These include empowering an existing regulator for a limited time period (Ofcom would be a strong candidate, given its experience in upholding its current remit to tackle harmful or offensive content, in the context of TV and radio), or establishing a shadow body that can make the necessary preparations ahead of the new authority. Either approach will require cooperation with other regulators to ensure the new framework complements existing safeguards.

5.17 Alongside these options, the government is carefully considering the remits of existing regulators that may overlap with these new requirements and whether consolidation of these functions, or a broader restructuring of the regulatory landscape, would reduce the risk of duplication and minimise burdens on businesses. It is also important to consider where possible future regulatory functions to tackle other online harms may sit to ensure the institutional structures will endure.

5.18 The government will take steps to ensure that the regulator can command public confidence in its independence, impartiality, capability and effectiveness. For example, we will consider examples from other regulated sectors about how to ensure that any movement of staff between the regulator and companies in scope does not undermine the public's confidence in the regulator's independence, while also ensuring the regulator is able to attract staff with the right skills, knowledge and experience.

Consultation questions

Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

Question 9: What, if any, advice or support could the regulator provide to help businesses, particularly start-ups and SMEs, comply with the regulatory framework?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?

Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?

Powers and capabilities of the regulator

5.19 The relationship between companies and regulators is often asymmetric. In regards to online harms this asymmetry can only be overcome if the regulator has real expertise in the technologies, platforms and practices under regulation.

5.20 The new regulator will require the capacity to understand how online technology and platforms operate, and collect, analyse and act upon the relevant data submitted by companies whose services are in scope. It will also require sufficient capacity to undertake research and horizon scanning to ensure the regulatory requirements keep pace with innovation and the emergence of new harms.

5.21 The government intends the new regulator to quickly become cost neutral to the public sector. To recoup the set-up costs and ongoing running costs, the government is considering fees, charges or a levy on companies whose services are in scope. This could fund the full range of the regulator's activity, including setting and enforcing codes of practice, preparing transparency reports, and any education and awareness activities by the regulator.

Consultation questions

Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

6: Enforcement

Summary

- The regulator will have a range of enforcement powers to take action against companies that fail to fulfil their duty of care. These will include the power to issue substantial fines.
- We are consulting on which enforcement powers the regulator should have at its disposal, particularly to ensure a level playing field between companies that have a legal presence in the UK, and those who operate entirely from overseas.
- In particular, we are consulting on powers that would enable the regulator to disrupt the business activities of a non-compliant company, measures to impose liability on individual members of senior management, and measures to block non-compliant services.
- Companies will continue to be liable for the presence of illegal content or activity on their services, subject to existing protections.

6.1 The regulator will have a suite of powers to take effective enforcement action against companies that have breached their statutory duty of care. While the primary objective will be to drive rapid remedial action, when companies do not cooperate there will be serious consequences.

The regulator's enforcement powers

6.2 To be effective, the regulator must have enforcement powers that both incentivise companies to comply and are technically possible to implement. The regulator will use these powers in a proportionate manner, taking the impact on the economy into account. These powers must also be designed and used in a way that creates a level playing field, so that companies with a presence in the UK are not disproportionately penalised.

6.3 The potential sanctions for non-compliance need to:

- Incentivise companies to fulfil their obligations quickly and effectively.
- Apply effectively across different types of online companies, which vary enormously in size and revenue and may be based overseas.
- Be proportionate to potential or actual damage caused and the size and revenue of the company.

6.4 There are a number of enforcement powers that will be an essential part of the new regulator's toolkit. These powers have been well tested in numerous other regulatory regimes. These core powers will include:

- Issuing civil fines for proven failures in clearly defined circumstances. Civil fines can be tied into metrics such as annual turnover, volume of illegal material, volume of views of illegal material, and time taken to respond to the regulator.
- Serving a notice to a company that is alleged to have breached standards, and setting a timeframe to respond with an action plan to rectify the issue.
- Requiring additional information from the company regarding the alleged breach.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Publishing public notices about the proven failure of the company to comply with standards.

6.5 However, because of the particularly serious nature of some of the harms in scope, the global nature of many online services and the weak economic incentives for companies to change their behaviour, we think it is likely the regulator will need additional powers at its disposal. These measures will be more contentious because of either challenges around their technical feasibility or the potential impact on companies and the wider economy. We are therefore consulting on these options alongside this White Paper:

- Disruption of business activities. In the event of extremely serious breaches, such as a company failing to take action to stop terrorist use of their services, it may be appropriate to force third party companies to withdraw any service they provide that directly or indirectly facilitates access to the services of the first company, such as search results, app stores, or links on social media posts. These measures would need to be compatible with the European Convention on Human Rights.
- ISP blocking. Internet Service Provider (ISP) blocking of non-compliant websites or apps – essentially blocking companies' platforms from being accessible in the UK – could be an enforcement option of last resort. This option would only be considered where a company has committed serious, repeated and egregious violations of the outcome requirements for illegal harms, failing to maintain basic standards after repeated warnings and notices of improvement. Deploying such an option would be a decision for the independent regulator alone. While we recognise that this would have technical limitations, it could have sufficient impact to act as a powerful deterrent. The British Board of Film Classification (BBFC) will have this power to address non-compliance when the requirements for age verification on online pornography sites come into force. We are exploring a range of options in this space, from a requirement on ISPs to block websites or apps following notification by the regulator, through to the regulator issuing a list of companies that have committed serious, repeated and egregious violations, which ISPs could choose to block on a voluntary basis.
- Senior management liability. We are exploring possible options to create new liability for individual senior managers. This would mean certain individuals would be held personally accountable in the event of a major breach of the statutory duty of care. This could involve personal liability for civil fines, or could even extend to criminal liability. In financial services, the introduction of the Senior Managers & Certification Regime has driven a culture change in risk management in the sector. Another recent example of government action is establishing corporate offences of failure to prevent the criminal facilitation of tax evasion. Recent changes to the Privacy and Electronic Communications Regulations (PECR) provide powers to assign liability to a specific person or position within an organisation. However, this is as yet largely untested. There are a range of options for how this could be applied to companies in scope of the online harms framework, and a number of challenges, such as identifying which roles should be prescribed and whether this can be proportionate for small companies.

Consultation questions

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Working with law enforcement and other relevant government agencies

6.6 As previously set out, the regulator will set a spectrum of expectations for companies, reflecting the nature of online harms and the company concerned. The expectations placed on firms, as set out in codes of practice, will vary according to the category of harm.

6.7 The codes of practice for specific illegal harms (e.g. terrorism and CSEA) will seek to set out expectations that keep pace with criminal behaviours and activities. They will establish requirements and processes, where appropriate and proportionate, for referring illegal content and activities to law enforcement and other relevant government agencies to aid investigations.

6.8 In formulating the codes of practice for other illegal harms, the regulator will be expected to incorporate insights from law enforcement and other relevant government agencies to ensure the codes are adequately addressing the threat. The regulator will also be required to ensure its wider actions are not detrimental to matters of national security.

Enforcement in an international context

6.9 The new regulatory regime will need to handle the global nature of both the digital economy and many of the companies in scope. The law will apply to companies that provide services to UK users. We will design the regulator's powers to ensure that it can take action against companies without a legal presence in the UK, including blocking platforms from being accessible in the UK as a last resort. Where companies do not have a legal presence in the UK, close collaboration between government bodies, regulators and law enforcement overseas, in the EU and further afield, will be required.

6.10 We are also considering options for the regulator, in certain circumstances, to require companies which are based outside the UK to appoint a UK or EEA-based nominated representative. This is similar to the concept of nominated representatives within the EU's GDPR. Under GDPR, if an organisation is based outside of the EEA but serves users in the EEA, they are required to nominate an EEA-based representative, notionally helping to enforce compliance in respect of companies established outside the EEA. This may be done by appointing a representative under a simple service contract, and for the information to be easily accessible to the regulator by publishing on the company's website. The regulator will also ensure that such representatives are tightly linked to their own genuine knowledge and ability to control the situation. However, under GDPR, the extent of compliance by companies based outside the EEA is still relatively untested – last year, the ICO launched the first extra-EEA enforcement case under the GDPR against AggregateIQ Data Services Ltd (AIQ) based in Canada. The regulator will take a company's failure to comply with such a requirement into consideration when making decisions about appropriate enforcement action.

6.11 It is vital that the regulator takes an international approach. Where similar regulators and legal systems are in place in other countries, the regulator will lead engagement with its international counterparts. Having these relationships will support the UK's ability to put pressure on companies whose primary base is overseas.

6.12 As part of our global strategy for tackling online harms, the government will seek to work with international partners to build consensus and identify common approaches to keep citizens safe online.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Appeals

6.13 Companies and others must have confidence that the regulator is acting fairly and within its powers. They will have the ability to seek judicial review of the regulator's actions and decisions through the High Court. We will also seek views through the consultation about whether there should be another statutory mechanism of review, which would allow the use of a tribunal other than the High Court, and what bar should be set for appeals through this route.

Consultation questions

Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

Question 14: In addition to judicial review, should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

> Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?
>
> Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

Current liability for illegal content

6.14 Under the current liability regime, which is derived from the EU's e-Commerce Directive, platforms are protected from legal liability for any illegal content they 'host' (rather than create) until they have either actual knowledge of it or are aware of facts or circumstances from which it would have been apparent that it was unlawful, and have failed to act 'expeditiously' to remove or disable access to it. In other words, they are not liable for a piece of user-generated illegal content until they have received a notification of its existence, or if their technology has identified such content, and have subsequently failed to remove it from their services in good time.

6.15 In 2018, the Prime Minister announced the government's intention to look at how existing frameworks and definitions can be made to work better, with a view to ensuring companies take greater responsibility for removal of illegal content on their services. The Prime Minister noted that applying 'publisher' levels of liability to companies would not be proportionate; such an approach would force companies to check every piece of content before upload to ensure it was legal, with implications for freedom of expression, and it would be difficult to reconcile with platforms hosting large amounts of user generated content.

6.16 Our review found that, while it is important to ensure that companies have the right level of liability for illegal content, this is not the most effective mechanism for driving behavioural change by companies. The existing liability regime only forces companies to take action against illegal content once they have been notified of its existence. It therefore does not provide a mechanism to ensure proactive action to identify and remove content. In addition, even if reforms to the liability regime successfully addressed the problem of illegal content, they would not address the full range of harmful activity or harmful behaviour in scope. More fundamentally, the focus on liability for the presence of illegal content does not incentivise the systemic improvements in governance and risk management processes that we think are

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

necessary. We concluded that standalone changes to the liability regime would be insufficient. Instead, the new regulatory framework takes a more thorough approach. It will increase the responsibility that services have in relation to online harms, in line with the existing law that enables platforms to operate. In particular, companies will be required to ensure that they have effective and proportionate processes and governance in place to reduce the risk of illegal and harmful activity on their platforms, as well as to take appropriate and proportionate action when issues arise. The new regulatory regime will also ensure effective oversight of the take-down of illegal content, and will introduce specific monitoring requirements for tightly defined categories of illegal content.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

7. Fulfilling the duty of care

Summary

- Ahead of the implementation of the new regulatory framework, we will encourage companies to take early action to address online harms.
- To assist this, the White Paper sets out high-level expectations of companies, including some specific expectations in relation to certain harms. We expect the regulator to reflect these in future codes of practice.

7.1 While it will be for the new regulator to produce codes of practice when it becomes operational, the government expects companies to take action now to tackle harmful content or activity on their services. For those harms where there is a risk to national security or to the physical safety of children, the government will publish interim codes of practice.

7.2 To support early action from companies, and to guide the initial priorities of the regulator, we have set out high-level expectations of companies below. Some of these apply to all harms in scope, and others apply to specific issues where a tailored response is more appropriate.

7.3 Given the range of services in scope of the regulatory framework, some of the expectations below may not be applicable to every company. However, each company in scope will be required to build an understanding of the risk associated with its service(s) and take reasonable steps to guard against the risk of harm in order to fulfil its duty of care.

The duty of care

7.4 As indication of their compliance with their overarching duty of care to keep users safe, we envisage that, where relevant, companies in scope will:

- Ensure their relevant terms and conditions meet standards set by the regulator and reflect the codes of practice as appropriate.
- Enforce their own relevant terms and conditions effectively and consistently.
- Prevent known terrorist or CSEA content being made available to users.
- Take prompt, transparent and effective action following user reporting.
- Support law enforcement investigations to bring criminals who break the law online to justice.
- Direct users who have suffered harm to support.
- Regularly review their efforts in tackling harm and adapt their internal processes to drive continuous improvement.

7.5 To help achieve these outcomes, we expect the regulator to develop codes of practice that set out:

- Steps to ensure products and services are safe by design.
- Guidance about how to ensure terms of use are adequate and are understood by users when they sign up to use the service.
- Measures to ensure that reporting processes and processes for moderating content and activity are transparent and effective.
- Steps to ensure harmful content or activity is dealt with rapidly.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Processes that allow users to appeal the removal of content or other responses, in order to protect users' rights online.
- Steps to ensure that users who have experienced harm are directed to, and receive, adequate support.
- Steps to monitor, evaluate and improve the effectiveness of their processes.

7.6 The rest of this chapter sets out more specific outcomes for harms in scope, as well as further examples of how companies will be expected to fulfil their duty of care.

CSEA

7.7 CSEA online poses a severe threat to the physical safety and emotional wellbeing of children. Companies will be required to take stringent action – proactive and reactive – to monitor and address the growing and evolving threat and to tackle all manifestations of CSEA activity, including bearing down on the proliferation of imagery and taking necessary steps to target grooming and live streaming.

7.8 We will also expect the regulator to set expectations around imagery that may not be visibly illegal, but linked to CSEA, for example, a series of images, some of which were taken prior to or after the act of abuse itself. We are continuing to work with partners to understand the impact of this abusive content on victims.

7.9 Existing legal requirements and voluntary industry initiatives are set out earlier in this White Paper.

CSEA: Fulfilling the duty of care

7.10 Some of the areas we expect the regulator to include in a code of practice are:

- The reasonable steps companies should take to proactively prevent new and known CSEA content, and links to such material, being made available to users.
- The reasonable steps companies should take to proactively identify and act upon CSEA activity such as grooming.
- The reasonable steps companies should take to proactively identify and act upon CSEA activity alongside, or within, live streams.
- The reasonable steps companies should take to proactively identify accounts showing indicators of CSEA activity and ensure children are protected from them, including disabling accounts and informing law enforcement where appropriate.
- The reasonable steps companies should take to prevent searches linking to CSEA activity and content, including automatic suggestions for CSEA content not being made and users being directed towards alternative sources of information or support.
- The reasonable steps companies should take to ensure services are safe by design.
- The reasonable steps companies should take to provide effective systems for child users, and their parents or carers, to report, remove and prevent further circulation of images of themselves which may fall below the illegal threshold, but which leave them vulnerable to abuse.
- The reasonable steps companies should take to implement effective measures to identify which users are children, and adopt enhanced safety measures for these users.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- The reasonable steps companies should take to promptly inform law enforcement where there is information about a CSEA offence, including provision of sufficient identifying information about victims and perpetrators.
- Steps companies should take to continually review their efforts in tackling CSEA, to adapt their internal processes and technology, and to continue to keep sufficiently up to date with the threat landscape; ensuring that their identification and response continually improves.
- Guidance on the CSEA content and activity companies should proactively prevent, identify and act upon, which will help inform the design and implementation of technological tools.
- Thresholds for the types of content companies should preserve following removal, for how long they should keep it and when/with whom such information should proactively be shared.
- Steps to ensure that users who are affected by CSEA content and activity are directed to, and are able to access, adequate support.

Terrorist use of the internet

7.11 Our aim is to ensure there is no safe space online for terrorists to operate, and to prevent the dissemination of terrorist content online. Such material can have significant real-world ramifications and poses a severe threat to national security. Given this, the regulator will require companies to take robust action to tackle terrorist content and activity on their services, and ideally prevent this content from reaching users in the first place.

7.12 We set out some of the existing measures to tackle terrorist use of the internet in Part 1. The establishment of the GIFCT and voluntary cooperation between the government and the industry has led to the positive creation and adoption of automated technologies by the biggest companies to proactively detect and remove terrorist content. This is essential if the threat from terrorists is to be prevented. It is also essential that smaller companies receive sufficient support to successfully prevent their platforms from being exploited, and that all relevant platforms support the role of law enforcement and other relevant government agencies.

Preventing terrorist use of the internet: Fulfilling the duty of care

7.13 Some of the areas we expect the regulator to include in a code of practice are:

- The reasonable steps companies should take to prevent new and known terrorist content, and links to content, being made available to users. This should include guidance on proactive use of technological tools, where appropriate, to identify, flag, block or remove terrorist content.
- Guidance on the content and/or activity companies should proactively prevent from being made available to users, which will help inform the design of technological tools.
- Clarification as to what constitutes an expedient timeframe for the removal of terrorist content where either it is not known that it is terrorist content at the point of upload, or it is not possible to prevent it from being made available to users.
- Guidance about the requirements for how companies should inform and support law enforcement and other relevant government agencies' investigations and prosecution of criminal offences in the UK. This will include specific guidance

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

about the content companies should preserve following removal and for how long, and when companies should proactively alert law enforcement and other relevant government agencies to this content.

- The reasonable steps companies should undertake when dealing with accounts that have uploaded, engaged with or disseminated terrorist content, including disabling accounts.
- The reasonable steps companies should take to identify and act upon terrorist activity or content, including within live streams.
- The reasonable steps we expect services to take to prevent searches which lead to terrorist activity and/or content, including automatic suggestions for terrorist content not being made and users being directed towards alternative sources of information or support.
- Steps companies should take to ensure that services are safe by design.
- Steps companies should take to continually review their efforts in tackling terrorist material, to adapt their internal processes and technology, and to continue to keep sufficiently up to date with the threat landscape; ensuring that their identification and response continually improves.

Serious violence

7.14 Violent content ranges from content which directly depicts or incites acts of violence, through to content which is violent with additional contextual understanding or which is harmful to users through the glamorisation of weapons and gang life.

Serious violence: Fulfilling the duty of care

7.15 Some of the areas we expect the regulator to include in a code of practice are:

- Guidance to companies to outline what activity and material constitutes violent or violence related content, including that which is explicitly criminal and how to report it.
- Guidance on the content and/or activity companies should proactively identify, to either prevent it being made publicly available or prevent further sharing and to ensure that users will not receive recommendations to violent or violence related content.
- Clarification as to what constitutes an expedient timeframe for the referral and removal of content when it is either proactively identified or referred.
- Guidance about the requirements for how companies should inform and support law enforcement and other relevant government agencies' investigations and prosecution of criminal offences in the UK. This should include specific guidance about the content companies should preserve following removal and for how long, and when companies should proactively alert law enforcement and other relevant government agencies to this content.
- The reasonable steps companies should take when dealing with accounts that have uploaded, engaged with or disseminated violent or violence related content, including disabling accounts.
- Measures to ensure that reporting processes are fit for purpose to tackle this harm and are clear, visible and easy to use. Users should receive clear explanations of decisions taken.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Steps to ensure that services have effective and transparent processes for moderating this type of content and users are kept up to date with the progress of their report.
- Processes companies should have in place to ensure that users can appeal the removal of content or other responses, in order to protect users' rights online.
- Steps to ensure that users who have been exposed to violent or violence related material are directed to, and are able to access, adequate support.
- Steps companies should take to ensure that services are safe by design.
- Steps companies should take to continually review their efforts in tackling this content, and to continue to keep sufficiently up to date with the threat landscape, adapting their internal processes accordingly to ensure that their identification and response continually improves.

Hate crime

7.16 Hate crimes include crimes demonstrating hostility on the grounds of an individual's actual or perceived race, religion, sexual orientation, disability or transgender identity. In Action Against Hate, the government's plan for tackling hate crime (2016), and Action Against Hate Two Years On (2018), jointly led by the Ministry of Housing, Communities and Local Government (MHCLG) and the Home Office, the government has made clear that offending online is just as serious as that occurring offline and perpetrators of hateful attacks should be held accountable for their actions. Companies should create platforms where people – whatever their identity or background – can work, learn and socialise together, with shared rights, responsibilities and opportunities.

7.17 A number of third party organisations are providing support to users to report instances of hate crime. The government supports True Vision, the police hate crime reporting portal, which helps encourage victims of hate crime to report instances online through their website report-it.org.uk. In Action Against Hate Two Years On (2018), we committed to supporting the National Police Chiefs' Council (NPCC) to refresh the True Vision website.

7.18 MHCLG and the Home Office also support and engage with third party organisations such as the Community Security Trust, Tell MAMA and Stop Hate UK, who have Trusted Flagger status with social media platforms to provide greater support to users to report experiences of hate crime online. We support the continued close cooperation of these organisations with government and social media platforms.

Hate crime: Fulfilling the duty of care

7.19 Some of the areas we expect the regulator to include in a code of practice are:

- Guidance to companies to outline what activity and material constitutes hateful content, including that which is a hate crime, or where not necessarily illegal, content that may directly or indirectly cause harm to other users – for example, in some cases of bullying, or offensive material.
- Guidance on the content and/or activity companies should proactively identify, to either prevent it being made publicly available or prevent further sharing.
- Steps companies should take to ensure their services are safe by design.
- Expectations around clear and accessible guidance to users on what constitutes hate crime and how to report it.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Measures to ensure that reporting processes are fit for purpose to tackle this harm and are clear, visible and easy to use. Users should receive clear explanations of decisions taken.
- Steps to ensure that services have effective and transparent processes for moderating this type of content and users are kept up to date with the progress of their report.
- Clarification as to what constitutes an expedient time frame for the removal of (or temporarily limiting access to) hateful content.
- Processes companies should have in place to ensure that users can appeal the removal of content or other responses, in order to protect users' rights online.
- Reasonable steps to take to ensure that users will not receive recommendations to hateful or inappropriate content.
- Steps to ensure that users who have been exposed to hateful material are directed to, and are able to access, adequate support.
- Guidance on the requirements for how companies should support law enforcement and other relevant bodies' investigations where appropriate.
- An expectation that companies will continually review their efforts in tackling hateful material and adapt their internal processes accordingly, to drive continuous improvement.

Harassment

7.20 Being harassed online can be upsetting and frightening, and online harassment can amount to a criminal offence. Far too many people, from public figures to schoolchildren, have experienced this kind of behaviour. A poll conducted for Amnesty International found that 21% of the women surveyed in the UK (504 women) had experienced online harassment or abuse, with 17% having experienced this on social media.[69] There are many forms of abuse and some evidence suggests differences in the type of abuse experienced between men and women. Research suggests more women than men experience sexual forms of verbal abuse (21% compared to 9% of men), while more men than women experience offensive name calling (30% compared to 23%) and physical threats (12% compared to 8%).[70]

7.21 The cumulative impact of online misogyny undermines women's and girls' digital contributions, silencing their voices and reducing their visibility. As a result of abuse or harassment, 67% of women in the UK experienced a feeling of apprehension when thinking about using the internet or social media.[71]

Harassment: Fulfilling the duty of care

7.22 Companies will need to take robust action when there is evidence that users are being harassed or abused on their services. Companies will also need to respond quickly and proportionately if this activity emerges.

69 Amnesty International (2018). Toxic Twitter – Women's Experiences of Violence and Abuse on Twitter. Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-3/

70 Pew Research Centre (2017). Online Harassment. Available at: http://www.pewInternet.org/2017/07/11/online-harassment-2017/

71 NewStatesman (2017). Social media and the silencing effect: why misogyny online is a human rights issue. Available at: https://www.newstatesman.com/2017/11/social-media-and-silencing-effect-why-misogyny-online-human-rights-issue

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

7.23 Current measures taken by companies to tackle online harassment include:

- Tools to report incidents of harassment.
- Tools to block or stay hidden from other users.
- Removal of content which is illegal or violates acceptable use.

7.24 Some of the areas we expect the regulator to include in a code of practice are:

- Steps companies should take to ensure that their services are safe by design. For victims of harassment, it is important that there are easy-to-use tools that allow them to take control over the privacy and visibility of their account and who is able to contact them.
- Tools companies can provide to help users experiencing harassment, such as the ability to mute, block or stay hidden from other users, and to manage and control access to particular services and content.
- Guidance about how to ensure it is easy for users to understand these tools, and the company's terms of use in relation to this harm, when they sign up to use the service.
- Measures to ensure that reporting processes are fit for purpose to tackle this harm, such as the ability to report a high volume of messages in bulk to reduce the burden on victims suffering from a campaign of harassment, and a prompt to use the tools to block the other user while the report is being investigated.
- Services have effective and transparent processes for moderating this type of content and activity. Users are kept up to date with the progress of their report.
- Steps companies should take to ensure harms are dealt with rapidly, such as removing content which is illegal, blocking users responsible for illegal activity and, where appropriate, supporting law enforcement efforts.
- Processes companies should have in place to ensure that users can appeal the removal of content or other responses, in order to protect users' rights online.
- Steps to prevent banned users creating new accounts to continue the harassment.
- Steps to limit anonymised users abusing their services, including harassing others.
- Steps to ensure that users who have experienced harassment are directed to, and are able to access, adequate support.

Disinformation

7.25 When the internet is deliberately used to spread false or misleading information, it can harm us in many different ways, encouraging us to make decisions that could damage our health, undermining our respect and tolerance for each other and confusing our understanding of what is happening in the wider world. It can also damage our trust in our democratic institutions, including Parliament.

7.26 Current initiatives that companies are exploring to tackle the spread of disinformation include:

- Terms of service that require users not to misrepresent their identity on social media in order to disseminate or amplify disinformation.
- Tools to report suspicious, fake or spam accounts on some social media platforms.
- Use of automated AI techniques to detect and remove fake and spam accounts.
- Partnerships between platforms and independent fact-checking services.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Tools to provide users with more context about the content they view on platforms, including enhanced transparency about the origins of political and electoral adverts.

Disinformation: Fulfilling the duty of care

7.27 Companies will need to take proportionate and proactive measures to help users understand the nature and reliability of the information they are receiving, to minimise the spread of misleading and harmful disinformation and to increase the accessibility of trustworthy and varied news content.

7.28 Some of the areas we expect the regulator to include in a code of practice are:

- The steps companies should take in their terms of service to make clear what constitutes disinformation, the expectations they have of users, and the penalties for violating those terms of service.
- Steps that companies should take in relation to users who deliberately misrepresent their identity to spread and strengthen disinformation.
- Making content which has been disputed by reputable fact-checking services less visible to users.
- Using fact-checking services, particularly during election periods.
- Promoting authoritative news sources.
- Promoting diverse news content, countering the 'echo chamber' in which people are only exposed to information which reinforces their existing views.
- Ensuring that it is clear to users when they are dealing with automated accounts, and that automated dissemination of content is not abused.
- Improving the transparency of political advertising, helping meet any requirements in electoral law.
- Reporting processes which companies should put in place to ensure that users can easily flag content that they suspect or know to be false, and which enable users to understand what actions have been taken and why.
- Processes for publishing data that will enable the public to assess the overall effectiveness of the actions companies are taking, and for supporting research into the nature of online disinformation activity.
- Steps that services should take to monitor and evaluate the effectiveness of their processes for tackling disinformation and adapt processes accordingly.

7.29 Maintaining a news environment where accurate content can prevail and high quality news has a sustainable future is vital to healthy social and democratic engagement, and key to long-term success in tackling disinformation. In March 2018, the government commissioned Dame Frances Cairncross to conduct her independent review into the sustainability of high quality journalism. In her detailed and considered report (published in February 2019), Dame Frances proposed that a 'news quality obligation' be imposed upon social media companies, which would require these companies to improve how their users understand the origin of a news article and the trustworthiness of its source. This recommendation is very much in line with our aim to strengthen the online environment and relates closely to our expectations for social media companies (as set out above). The government is now considering this proposal and Dame Frances' other recommendations, and we will look to take action where appropriate.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

7.30 Companies will be required to ensure that algorithms selecting content do not skew towards extreme and unreliable material in the pursuit of sustained user engagement.

7.31 Importantly, the code of practice that addresses disinformation will ensure the focus is on protecting users from harm, not judging what is true or not. There will be difficult judgement calls associated with this. The government and the future regulator will engage extensively with civil society, industry and other groups to ensure action is as effective as possible, and does not detract from freedom of speech online.

Encouragement of self-harm and suicide

7.32 Users should be able to talk online about sensitive topics such as suicide and self-harm, but more needs to be done to protect vulnerable users and tackle content and behaviour which encourages suicide and self-harm.[72]

7.33 Current measures to tackle the encouragement of self-harm and suicide include:

- Arrangements between individual companies and charities to improve the identification and removal of this content when it is reported.
- Services that signpost help and promote supportive content to their users.

Encouragement of self-harm and suicide: Fulfilling the duty of care

7.34 Companies will be required to take robust action to address harmful suicidal and self-harm content that provides graphic details of suicide methods and self-harming, including encouragement of self-harm and suicide. Services must also respond quickly to identify and remove content which is illegal or violates terms of use, and act swiftly and proportionately when this content is reported to them by users.

7.35 Some of the areas we expect the regulator to include in a code of practice are:

- Steps to ensure that vulnerable users and users who actively search for or have been exposed to this content, including content that encourages eating disorders, are directed to, and able to access, adequate support.
- Ensuring that companies work with experts in suicide prevention to ensure that their policies and practices are designed to protect the most vulnerable (and to ensure that moderators receive appropriate training).
- Steps companies should take to ensure that their services are safe by design, including tools to help users avoid material or behaviour which encourages suicide or self-harm, and measures to block content and block, mute and stay hidden from other users.
- Guidance about how to ensure it is easy for users to understand these tools, and the company's terms of use in relation to these harms, when they sign up to use the service.
- Processes to stop algorithms promoting self-harm or suicide content to users.
- Measures to ensure that reporting processes and processes for moderating content and activity are transparent and effective at tackling the encouragement of self-harm and suicide and measures to ensure that users are kept up to date with the progress of their report.

72 Encouraging and assisting suicide is a criminal offence. Self-harm is not a criminal offence.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Steps services should take to ensure they engage sufficiently with civil society groups and law enforcement, so that moderators are educated about what constitutes self-harm or suicide encouragement and how it can be prevented and tackled.
- Steps companies should take to ensure harm is tackled rapidly, such as removing content which is illegal or violates acceptable use, and blocking users responsible for activity which violates terms and conditions, as well as steps that services can take to ensure that these measures are conducted sensitively.
- Processes companies should have in place to ensure that users can appeal the removal of content or other responses, in order to protect users' rights online.
- Steps to prevent banned users creating new accounts to continue to encourage suicide or self-harm.

Online abuse of public figures: Fulfilling the duty of care

7.36 As set out in Box 14, those involved in public life in the UK experience regular and sustained abuse online, which goes beyond free speech and impedes individuals' rights to participate. As well as being upsetting and frightening for the individual involved, this abuse corrodes our democratic values and dissuades good people from entering public life.

7.37 The steps we expect the regulator to include in codes of practice relating to all forms of abusive behaviour online, including harassment and cyber-bullying, will also help address this problem, and include:

- Steps companies should take to ensure that their services are safe by design. For all users, including public figures, it is important that there are easy-to-use tools that allow them to take control over the privacy and visibility of their account and who is able to contact them.
- Tools companies can provide to help users experiencing abuse, such as the ability to mute, block or stay hidden from other users, and to manage and control access to particular services and content.
- Clear guidance in the company's terms of use on the type of activity which will be treated as unacceptable and the actions the company will take in response to such activity, which is available to users when they sign up to use the service.
- Measures to ensure that reporting processes are fit for purpose to tackle this harm, such as the ability to report a high volume of messages in bulk to reduce the burden on victims suffering from a campaign of online abuse, and a prompt to use the tools to block the other user while the report is being investigated.
- Services have effective and transparent processes for moderating this type of content and activity. Users are kept up to date with the progress of their report.
- Steps companies should take to ensure harms are dealt with rapidly, such as removing content which is illegal, blocking users responsible for illegal activity, enforcing and upholding the service's relevant terms and conditions and, where appropriate, supporting law enforcement efforts.
- Processes companies should have in place to ensure that users can appeal the removal of content or other responses, in order to protect users' rights online.
- Steps companies should take to limit anonymised users using their services to abuse others.
- Steps to prevent banned users creating new accounts to continue the abuse.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Steps to ensure that users who are affected by abusive comments and activity are directed to, and are able to access, adequate support.

Interference with legal proceedings

7.38 Activity that can impede a person's right to a fair trial, or that breaches a person's legal right to anonymity, such as communications that may amount to a breach of a court order or a statutory prohibition, or that may prejudice a jury, may amount to contempt of court or be a criminal offence.

7.39 Current measures to tackle this problem include:

- Action taken by law enforcement and the criminal justice system in relation to publishing information online and exposing the identity of protected individuals which could jeopardise legal proceedings.
- The bringing of contempt proceedings against those who create a substantial risk of serious prejudice.

7.40 Furthermore, in its Response to the Call for Evidence on the Impact of Social Media on the Administration of Justice,[73] the Attorney General's Office has:

- Set out plans to promote the safe use of social media as part of a public legal education campaign, which will include a GOV.UK webpage.
- Highlighted that the Judicial Office are working to develop clear, accessible, and comprehensive guidance on contempt.
- Agreed points of contact with a number of social media companies so that relevant material can be flagged and, if necessary, removed.
- Set out plans to work with cross-government partners to improve the enforcement of the law on anonymity online.

7.41 Companies will be required to take robust action when there is evidence that a risk of interference with criminal trials or other legal proceedings is present. Companies will also be required to respond quickly and proportionately where new risks emerge.

Interference with legal proceedings: Fulfilling the duty of care

7.42 Some of the areas we expect the regulator to include in a code of practice are:

- Tools companies can provide to help users report possible interference with legal proceedings, such as the ability to report anonymously.
- Measures to ensure that reporting processes and processes for moderating content and activity are transparent and effective at tackling interference with legal proceedings and measures, to ensure that users are kept up to date with the progress of their report.
- Steps companies should take to ensure harms are dealt with rapidly, to ensure that posts that are in contempt of court or that breach anonymity orders are removed as soon as possible once they have been reported. User guidance setting this out should be incorporated into the company's terms and conditions to ensure clarity when users sign up to use the service.

73 Attorney General's Office (2019). Response to Call for Evidence on the Impact of Social Media on the Administration of Justice. Available at: https://www.gov.uk/government/publications/response-to-call-for-evidence-on-the-impact-of-social-media-on-the-administration-of-justice

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Processes companies should have in place to ensure that users can appeal the removal of content or other responses, in order to protect users' rights online.
- Steps to prevent banned users creating new accounts to continue or repeat the interference with legal proceedings.

Cyberbullying

7.43 Cyberbullying, including trolling, is unacceptable. Being bullied online can be a deeply upsetting experience, particularly for children or other vulnerable users.

7.44 Current measures to tackle cyberbullying and trolling include:

- Provision of information and resources on bullying and other online safety issues.
- Tools to report incidents of bullying.
- Tools to block or stay hidden from other users.
- Removal of content which violates acceptable use.

Cyberbullying: Fulfilling the duty of care

7.45 The regulator will set out steps that should be taken to tackle cyberbullying, such as ensuring that those who have suffered from this harm are directed to, and are able to access, adequate support.

7.46 In the meantime, the statutory Social Media Code of Practice, published alongside this White Paper in line with the DCMS Secretary of State's duty under section 103 of the Digital Economy Act 2017, sets out non-binding principles that companies should adhere to in order to tackle bullying, insulting, intimidating and humiliating conduct online. It also explains good practice ways to implement these principles. We expect all social media companies to adhere to this code of practice, ahead of the new regulatory requirements. We expect the regulator to consider this guidance when drawing up future codes of practice.

7.47 These principles are:

- Social media providers should maintain a clear and accessible reporting process to enable individuals to notify social media providers of harmful conduct.
- Social media providers should maintain efficient processes for dealing with notifications from users about harmful conduct.
- Social media providers should have clear and accessible information about reporting processes in their terms and conditions.
- Social media providers should give clear information to the public about action they take against harmful conduct.

Children accessing inappropriate content

7.48 Some online content that is lawful and appropriate for adults, such as dating apps or pornography, may cause significant harm to children who either access it intentionally or stumble across it. The Chief Medical Officers for England, Wales and Scotland recently advocated a precautionary approach to protecting children from harmful content because of its possible impact on their mental health or development.

7.49 Current measures to tackle children accessing inappropriate content include:

- Forthcoming compulsory age verification for commercial online pornography sites.
- Family friendly filters to filter inappropriate material.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Content warnings for inappropriate content.

7.50 The designated classification authorities for offline content, the BBFC and the Video Standards Council (VSC), have clear standards based on their evaluation of likely harm and use these to allocate BBFC or PEGI age suitability ratings to inform viewing decisions and protect children and vulnerable adults. These age ratings are applied voluntarily to online content by some publishers and platforms. The new regulatory framework is not intended to impact the existing classification of offline and online content by BBFC and VSC.

Children accessing inappropriate content: Fulfilling the duty of care

7.51 Companies will be required to take robust action when there is evidence that children are accessing inappropriate content. Companies will also be required to respond quickly and proportionately where new risks emerge.

7.52 Some of the areas we expect the regulator to include in a code of practice are:

- Steps companies should take to ensure that their services are safe by design. This could include the provision of accounts with different settings for children.
- Terms of service should make clear what behaviour and activity is tolerated on the service and the measures that are in place to prevent children accessing inappropriate content and they should be easy for children and parents to understand.
- Steps companies should take to ensure children are unable to access inappropriate content, including guidance on age verification, content warnings and measures to filter and block inappropriate content.
- Measures to ensure that reporting processes are fit for purpose to tackle this harm and are clear, visible and easy for children and parents to understand. Users should receive clear explanations of decisions taken.
- Services have effective and transparent processes for moderating this type of content and activity. Users are kept up to date with the progress of their report.
- Steps companies should take to ensure harms are rapidly dealt with, such as removing content which violates terms of service.
- Processes services should have in place to ensure that users can appeal the removal of content or other responses, in order to protect users' rights online.
- Steps to prevent banned users creating new accounts in order to continue to make inappropriate content which violates terms of service.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

PART 4: Technology, education and awareness

8: Technology as part of the solution

Summary

- Companies should invest in the development of safety technologies to reduce the burden on users to stay safe online.
- In November 2018, the Home Secretary co-hosted a hackathon with five major technology companies to develop a new tool to identify online grooming, to be licensed for free to other companies, but more of these innovative and collaborative efforts are needed.
- The government and the new regulator will work with leading industry bodies and other regulators to support innovation and growth in this area and encourage the adoption of safety technologies.
- The government will also work with the industry and civil society to develop a safety by design framework, linking up with existing legal obligations around data protection by design and secure by design principles, to make it easier for start-ups and small businesses to embed safety during the development or update of products and services.

8.1 Technology can play a crucial role in keeping users safe online. By designing safer and more secure online products and services, the tech sector can equip all companies and users with better tools to tackle online harms. We want the UK to be a world-leader in the development of online safety technology and to ensure companies of all sizes have access to, and adopt, innovative solutions to improve the safety of their users.

Existing initiatives

8.2 In the UK, a dynamic and innovative market has sprung up around online safety, developing tools for business to protect their users from harms. For example:

- SuperAwesome, one of the fastest-growing technology SMEs in the UK, provides tools and technology that protect the digital privacy of children.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Crisp, an SME with complex AI-based tools to support moderation and monitoring of content, helps hundreds of companies worldwide run safer platforms – every month its systems assess billions of pieces of content for illegal or harmful content, and help to identify repeat offenders who are continually posting inappropriate content.
- Yoti, a digital identity provider, is partnering with the Yubo social network to use machine learning age estimation to detect whether website users are in the right age band for their platform – an important step in helping safeguard children online.

8.3 The government is supporting the development of this emerging safety tech ecosystem in the UK:

- The Home Office worked with Faculty (formerly ASI Data Science) to develop technology that can identify the official Daesh propaganda videos that are a key part of the terrorist groups efforts to radicalise, recruit and inspire acts of terrorism in the UK and abroad.
- The government launched a challenge fund, through the GovTech Catalyst scheme, to develop technology that can automate the detection of terrorist still imagery. Five UK companies have been awarded £50,000 to work on proposals, and this year the leading proposals will receive up to £500,000 to develop and test a prototype.
- The government is investing £300,000 to fund up to five innovative projects that use new technologies to disrupt live online CSEA.
- Through National Cyber Security Centre (NCSC) Accelerator programmes, the government is ensuring the rapid development of solutions to cyber security challenges such as authentication, mobile device security and identity management, that work to reduce online harms through increasing the security of users' online environments, giving them more control over their interactions and making access harder for those who seek to use technology to facilitate abuse.

Online safety apps: BBC Own It **Box 27**

BBC Own It, launching later in 2019, is a new wellbeing app aimed at children aged 8-13 receiving their first smartphone. The app is part of the BBC's commitment to supporting young people in today's changing media environment and follows the successful launch of the Own It website in 2018.

The app combines state-of-the-art machine learning technology to track children's activity on their smartphone with the ability for children to self-report their emotional state. It uses this information to deliver tailored content and interventions to help children stay happy and healthy online, offering friendly and supportive nudges when their behaviour strays outside the norm. Users can access the app when they're looking for help but it will always be on-hand to give instant, on-screen advice and support when they need it via a specially-developed keyboard. Features include:

- Reminding them to think twice before sharing personal details like mobile numbers on social media.
- Helping them understand how messages could be perceived by others, before they hit send.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Tracking their mood over time and offering guidance on how to improve the situation if needed.
- Information on topics like using phones late at night and the impact on their wellbeing.

The app features specially commissioned content from across the BBC. It provides useful material and resources to help young people get the most out of their time online, and build healthy online behaviours and habits. The app will help young people and parents have more constructive conversations about their experiences online, but won't provide reports or feedback to parents and no data will leave their device.

Tackling online grooming: industry hackathon **Box 28**

The challenge of online grooming of children for exploitation and abuse crosses borders and platforms. Addressing it requires collaboration between companies to develop innovative solutions that can be shared in a joint effort to eradicate grooming from digital space.

- In November 2018, the Home Secretary co-hosted a 'hackathon' event in the US with Microsoft and a range of other tech companies, where they worked to develop a new AI product to detect online grooming of children. Hackathon participants analysed tens of thousands of conversations to understand patterns used by predators. This enabled engineers to develop technology to automatically and accurately detect these patterns.
- During 2019, this anti-grooming tool will be licensed free of charge to smaller and medium-sized technology companies worldwide – and government will work closely with industry to help ensure high rates of adoption.

Boosting innovation in safety technology

8.4 The online safety ecosystem incorporates a number of distinct markets including third party technical solutions, human moderation services, hashing and finger-printing technologies and AI/machine learning solutions for the automated detection of harmful content. The government will work with the tech sector to make the UK a world-leader in innovative safety solutions across these markets.

8.5 The new regulator will use its unique position in the market to drive development of new technologies and encourage the sharing of tools and best practice amongst companies.

8.6 In the meantime, the government will work with partners across industry, academia and civil society to support innovation in safety technologies. In particular, we will:

- Assess the capability and potential of the UK online safety sector.
- Work with Tech Nation, TechUK and other industry partners to help companies more effectively detect and respond to online harms by promoting the rapid innovation, development and scale-up of safety products.
- Work with UKRI to support research into understanding online harms and the development of innovative technological solutions that meet the challenge of protecting citizens online.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Support the development of scalable privacy-enhancing technologies to allow companies to access training data to develop AI solutions, without compromising highly sensitive or illegal datasets.

8.7 We are bringing in external expertise to help government provide further direction. This includes the Digital Charter Fellowship programme, which DCMS is running in partnership with the Alan Turing Institute (Turing). Fellows will develop – with the lead government departments – policy responses to key challenges posed by the internet and new technologies. This will include experimenting with a range of processes and tools, including convening small groups of experts (from industry, academia and government) to work intensively on the issue. Manipulation, disinformation and online safety are key areas of focus for the first phase of the Fellowship programme.

8.8 We will work further with research organisations to understand how AI can best be used to detect, measure and counter online harms, while ensuring its deployment remains safe and ethical.

Online safety initiatives: Analysing and countering hate speech: The role of AI **Box 29**

Hateful content on digital platforms is a growing problem in the UK, inflicting harm on victims, creating and exacerbating social divisions, and eroding trust in the host platforms.

- However, despite the harm caused by hate content, we lack adequate data on its scale and scope, limiting our ability to develop more sophisticated and effective responses. Part of the challenge is that online hate takes many forms and is directed against many different targets, including ethnic minorities and women.
- A new project led by Turing is setting out to address this issue. The 'Hate Speech: Measures and Counter-measures' project will use a mix of natural language processing techniques and qualitative analyses to create tools which identify and categorise different strengths and types of online hate speech.
- The aim is to make these tools open and accessible to the public, and ultimately for them to be used to support a broad range of commercial and public sector providers to detect and address harmful and undesirable content. The project also aims to release annotated training datasets, enabling other researchers to further build on their work.
- Turing is planning work more broadly to study the influence of algorithmic systems on humans, as part of its initiative on safe and ethical AI.

Interventions to boost adoption and use of technologies

8.9 Many of the leading companies already use their resource and expertise to support the development of shared platforms and technologies that can be adopted by wider industry. These include Microsoft's PhotoDNA, a shared system for detecting and responding to images of child sexual abuse, and Google's Perspective API, which uses machine learning to flag potentially harmful or 'toxic' content to moderators. In November 2018, Microsoft and other companies came together in a 'hackathon' to develop anti-grooming technology, which will be licensed free of charge to smaller companies worldwide (Box 28).

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

8.10 It is crucial that we continue to drive the adoption of safety products so that users receive consistent levels of protection online. To achieve this we will:

- Work with industry to encourage the development and take-up of free or low-cost shared platforms for safety, such as the Home Office anti-grooming tool.
- Fund research by Doteveryone, an independent thinktank, into barriers to the adoption of technologies and working practices that promote user safety and wellbeing, and the practical guidance and techniques needed to overcome these barriers.
- Support the development by Innovate UK and BSI of a publicly available standard (PAS) for responsible innovation, to help companies think through and identify any potential issues raised by their proposed innovations.

Safety by Design

8.11 Creating a safer user experience on online products and platforms requires more than the use of new technology. Decisions made throughout the product development life cycle – around privacy and data protection, cybersecurity, moderation, reporting and support mechanisms for users, clarity of terms and conditions – all combine to shape the overall safety and security of a user's experience.

8.12 To prepare for the new regulatory framework, it should be as easy as possible for designers of products and platforms to understand what standards are expected of them, and to be able to incorporate existing good practices into their products from the earliest stages of product development to ensure that their products are safe by design.

8.13 Box 30 provides an example of good practice safe design that aims to protect children online. Across the industry as a whole, however, standards remain inconsistent, and frequently do not prioritise users' rights – in particular, it is commonplace for design to encourage addictive behaviour rather than wellbeing, or for collecting user-data to be prioritised over privacy. This results in an unacceptable burden on users to manage their online safety without sufficient support from the companies that they rely on. This is a particular concern for vulnerable users.

Online safety apps: Lego Life **Box 30**

In 2017, the LEGO Group launched a social-themed app, LEGO® Life. The ambition behind the app is to inspire younger children to build and share their creations in a high-safety, high-trust environment. LEGO® Life embeds safety by design principles, as well as introducing children to positive elements of social platforms, such as being able to share moments with family and friends.

They have recently strengthened this approach by using innovative solutions, such as the anthropomorphic advice engine, Captain Safety. The character provides a safety tutorial from the beginning and becomes the child's guide throughout the experience, delivering empowering safety messages at certain critical points, such as before sharing certain data or commenting on public posts.

8.14 To drive up standards, the government will work with industry and civil society to develop a Safety by Design framework to help companies incorporate online safety throughout the development or update of online services. This framework will set out clear principles and practical guidance on how to include online safety features in new applications

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

and platforms from the start, targeted at digital product teams, including designers, developers and user researchers. This could include guidance which highlights the need for providers to:

- Make it clear to users what forms of content are acceptable, as part of the terms of service and throughout their journey.
- Have effective systems for detecting and responding to illegal or harmful content, including the use of AI-based technology and trained moderators.
- Make it easy for users to report problem content, and design an efficient triage system to deal with reports.
- Give users control of their experience by collecting the minimum amount of personal data and giving them informed choices about how their personal information, including geolocation data, is used.

8.15 In developing the framework, we will pay special attention to the needs of start-ups and scale-up businesses, which can lack the capacity and expertise to ensure their products and services are safe by design. We expect the framework will be complementary with existing privacy by design and security by design standards. For example, it will reflect and signpost the forthcoming Age-appropriate design code (see Box 31) – and the Code of Practice for Consumer Internet of Things Security (Box 32).

8.16 We anticipate that the new regulator will build on this framework and use it to inform its approach to issuing codes of practice and guidance to companies about how to fulfil their new legal duties. We envisage that this framework will support companies to take practical action to tackle harm and meet the high-level expectations set out in Chapter 7.

8.17 The DfE is also planning to publish its Education Technology Strategy in the spring which will highlight the importance of privacy, security and safety. The strategy will include clarity on the guidelines that EdTech suppliers should adhere to and the guidance available for schools and colleges to support their procurement and use of safety technology.

Consultation questions

Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

Online safety initiatives: Age-appropriate design code: Safer design standards for children — **Box 31**

Whether playing online games, watching and sharing videos or interacting with friends via apps and social media, children today grow up with digital technology as a fundamental part of their daily lives. This can enrich their lives but it can also pose risks. To help guarantee a better digital future for our children, we need to have world-leading standards that provide proper safeguards for our children when online.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- The government included provisions in the Data Protection Act 2018 to help ensure this is the case. These require the Information Commissioner to produce an 'age-appropriate design code of practice', to provide guidance on the privacy standards that organisations should adopt where they are offering online services and apps that children are likely to access and which will process their data.
- These standards in the code will be backed by legally enforceable data protection laws, which empower the Information Commissioner to take action and impose tough penalties under GDPR, including enforcement orders and fines of up to 4% of global turnover.
- The code will focus on the best interests of a child. It will ensure nothing is left to chance and that a 'data protection by design' approach is adopted. Companies will be held accountable for their actions living up to their promises on how they handle children's information.
- The code will address the need to implement high privacy settings by default and use language that is clear and easy to understand for youngsters at different stages of their development. It will also focus on key safeguards around the automated profiling of children, the use of geolocation data, and the transparency of marketing techniques.
- It will also address practices such as those used by sites and apps to personalise a child's experience to encourage them to stay online longer, such as auto-play videos and the timing of social media notifications.
- Work on developing the code is well advanced, with calls for evidence and commissioned research already concluded. A formal public consultation will follow in the coming months.

Online safety initiatives: Internet of Things: Security Code of Practice **Box 32**

Recent years have seen huge growth in the number of 'Internet of Things' (IoT) products, consumer-facing internet connected 'smart' devices that people use in their homes such as smart appliances, personal assistants, children's toys, web cameras and baby monitors. However, across the IoT, there are many instances of insecure products that make consumers vulnerable to cyber attacks, which can lead to physical and emotional harm.

- To combat this, in October 2018 the government published the Code of Practice for Consumer IoT Security. This code of practice consists of thirteen outcome-focused guidelines that clearly describe the steps that IoT producers need to take to ensure their products and services are secure by design.
- We believe the next stage in this work is for appropriate aspects of the code of practice to become legally enforceable, therefore offering consumers greater protection from the online harms associated with these products. We have commenced work to consider which aspects of regulatory change are necessary.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- The code of practice has also been used to create the first globally-applicable industry standard for IoT consumer devices, the ETSI 103 645 Technical Standard (ETSI TS). We will work to drive adoption of this standard, setting in place a harmonised technical approach that protects citizens across the world.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

9. Empowering users

Summary

- Users want to be empowered to manage their online safety, and that of their children, but there is insufficient support in place and they currently feel vulnerable online.
- Government has taken steps to address digital literacy in the relevant areas of the school curriculum.
- The Government will develop a new online media literacy strategy, through broad consultation with stakeholders.
- While companies are supporting a range of positive initiatives, there is insufficient transparency about the level of investment and the effectiveness of different interventions. The new regulator will have the power to require companies to report on their education and awareness raising activities.

9.1 All users, children and adults, should be empowered to understand and manage risks so that they can stay safe online. The government is ensuring that children get high quality education at school to develop their digital literacy. Adult users should act in an acceptable manner, challenge unacceptable behaviour when they witness it, and use tools available to them to manage their online experience. They have a responsibility to manage their own online safety, and to support children in their care. In this rapidly changing environment, it can take time to learn how to evaluate what is and is not risky, and to acquire the skills to avoid harm.

9.2 Many companies have invested in education and awareness activities, often in partnership with civil society, and created tools to empower their users, such as software from Apple and Google that produces reports for users that help them to assess and control their online activity (see Box 33). While such industry initiatives are welcome, there continues to be a lack of transparency about their scale and effectiveness, and a real risk of duplication in the absence of strategic coordination. While we recognise the concerns of civil society about the risks of disrupting these existing positive working relationships with industry, we want to work with all stakeholders to ensure that there is sufficient industry investment in education and preventative activity, and that there is independent evaluation of its effectiveness.

9.3 The technical complexity and pace of innovation of the online world means that there is a constant need to improve the tools available to users so that they are able to manage and address risks online. A number of recent independent reports have also highlighted the specific need for improved digital literacy, including the DCMS Select Committee's report into disinformation[74] and the Cairncross report on A sustainable future for journalism.[75] Children have also told us that they want more education about online safety, as well as more support from tech companies to keep them safe (see Box 34).

74 Digital, Culture, Media and Sport Committee (2019). Disinformation and 'fake news': Final Report. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

75 The Cairncross Review (2019). A sustainable future for journalism. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Online safety apps: Apple Screen Time and Google Family Link **Box 33**

In June 2018, Apple launched updates to its mobile operating system that help customers reduce interruptions and manage screen time for themselves and their families.

These included:

- Daily and weekly reports that inform users of the total time spent in each app, usage across categories of apps, how many notifications are received and how often a person picks up their device.
- Tools to set specific limits on the amount of time spent in an app, and a notification that displays when a time limit is about to expire.
- Settings that allow users to more closely control their notifications, including a mode to help people get a better night's sleep.
- Parents can access information about their child's activity on their own devices to understand where their child spends their time and can manage and set limits for them.

Similarly, Google's Family Link app allows parents to:

- View how long their children spend on different apps.
- Approve or block apps their children want to download, or recommend specific apps.
- Set limits on screen time, and remotely lock a child's device for a break.

Furthermore, some gaming consoles, such as Xbox One, Playstation4 and Nintendo Switch have tools which allow parents to control access to content and place limits on screen time.

Online safety initiatives: Understanding children's needs online **Box 34**

The UK Council for Child Internet Safety (now the UK Council for Internet Safety) published the Children's online activities, risks and safety research review in October 2017. This included evidence that while many feel able to cope with general or random negative comments online, personal or targeted behaviour was more distressing and they were likely to seek help from friends or family, or report abuse to the relevant social media platform. However, when experiences are persistent and extreme, children can find it difficult to tell anyone, and this often makes the experience worse.

- Children and young people are much more likely to confide in friends than parents or carers about upsetting or embarrassing incidents. The review notes a range of reasons children and young people don't talk to parents, including feeling uncomfortable talking to parents or worries that devices and internet access will be taken away from them.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Alongside the Internet Safety Strategy Green Paper, the government worked with the British Computing Society (BCS), The Chartered Institute for IT, to carry out a survey of 6,500 children and young people about online safety.[76]

The survey highlighted that:

- Two thirds of children aged 12 and under (67%) and nearly half of 13 to 18 year olds (46%) would welcome more education in schools about online safety.
- Children have low expectations of social media platforms in relation to their privacy, safety and security online and would like to be better protected against abusive content.
- Nearly half (42% of under 13s, 41% of 13 to 18 year olds) said tech companies don't think about the online safety of people their age when they're making websites or apps.
- Nearly two thirds (66% of under 13s, 63% of 13 to 18 year olds) thought tech firms should proactively delete abusive messages before complaints are made.

Existing initiatives to empower users to stay safe online

9.4 DfE continues to incorporate online safety into the school curriculum, to help children and young people understand healthy relationships online, and to improve their digital literacy to equip them to manage the different and escalating risks that young people face.

9.5 As part of this, DfE is making Relationships Education compulsory for all primary pupils, Relationships and Sex Education compulsory for all secondary pupils and Health Education compulsory for all pupils in all primary and secondary state-funded schools in England. The Department recently consulted[77] on draft guidance for these subjects which includes teaching about respectful relationships, including online, as well as health and mental wellbeing. This will include:

- How to stay safe online.
- Critically considering information and how people present themselves online.
- Rights and responsibilities.
- How data is gathered, shared and used.
- The benefits of rationing time spent online.

9.6 In the government response to the above consultation, we also set out that we intend to produce supporting information for schools on how to teach about all aspects of internet safety, not just those relating to relationships, sex and health, to help schools deliver this in a coordinated and coherent way across their curriculum.

9.7 Schools will be encouraged to teach the new subjects from September 2019 – many of them are already doing this and will be able to adapt to the new guidance quite quickly. The requirement to teach the new subjects will then follow from September 2020.

76 BCS (2018). Young people want more from social media giants over online safety. Available at: https://www.bcs.org/more/about-us/press-office/press-releases/young-people-want-more-from-social-media-giants-over-online-safety-survey-by-bcs-reveals/

77 Department for Education (2019). Consultation outcome – Relationships (and sex) education and health education. Available at: https://www.gov.uk/government/consultations/relationships-and-sex-education-and-health-education

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

9.8 The new computing curriculum, introduced in September 2014, includes the principles of e-safety at all key stages, with progression in the content to reflect the different and escalating risks that young people face. This includes how to use technology safely, responsibly, respectfully and securely, how to keep personal information private, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

9.9 These changes to the curriculum are part of a broader strategy to ensure that schools are supporting young people to stay safe online. Some of the measures included in this strategy include:

- A National Centre for Computing Education that will develop, curate and disseminate a central repository of free, high quality, knowledge-rich resources for teachers to cover the whole computing national curriculum (from key stages 1-4).
- Strengthened statutory safeguarding guidance for schools in England, Keeping Children Safe in Education (KCSIE), including guidance on how to keep children safe online. The revised guidance came into effect on 3 September 2018.
- A new online safety working group, established by the Minister for Children and Families and made up of online safety and education experts, to advise the department on future iterations of the safeguarding guidance.

Wider initiatives to empower users to stay safe online

9.10 In Chapter 2, we set out the significant body of work being led by the UK Council for Internet Safety to ensure that children and vulnerable adults are taught about online safety, and that parents have access to appropriate advice, including an online resilience toolkit and driving the adoption of the Education for a Connected World framework[78] in schools (see Box 35). The government has also funded the UK Safer Internet Centre to develop cyberbullying guidance which provides advice for schools on understanding, preventing and responding to cyberbullying, and an online safety toolkit to help schools deliver sessions through PSHE about cyberbullying, peer pressure and sexting. There are a number of civil society organisations that have also made valuable contributions to online safety education and awareness, such as 5Rights (see Box 36).

9.11 The Information Commissioner's Office has also developed a public facing campaign to enable the public to better understand their data protection rights called 'Your Data Matters'.[79] The ICO has also produced teaching materials to support and empower children to understand their data rights.[80]

78 UKCIS (2018). Education for a Connected World framework. Available at:https://www.gov.uk/government/publications/education-for-a-connected-world

79 ICO. Your data matters – building confidence and trust. Available at: https://ico.org.uk/for-organisations/resources-and-support/your-data-matters-campaign/

80 ICO. Resources for schools. Tailored lesson plans for children and young people. Available at: https://ico.org.uk/for-organisations/education/resources-for-schools/

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Online safety initiatives: Education for a Connected World **Box 35**

The UK Council for Internet Safety's (UKCIS) Education for a Connected World framework describes the digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives.

Designed to help educators engage in a meaningful dialogue with their students about their lives online, the tool covers a wide range of issues, including self-image and identity, privacy and security, online relationships and online bullying.

Online safety initiatives: 5Rights **Box 36**

The 5Rights Foundation is a registered charity that produces child-led and co-designed policies and works towards an online environment that meets the needs and protects the rights of children and young people online.

The 5Rights framework takes existing children's rights and applies them to the digital world:

- The Right to Remove
- The Right to Know
- The Right to Safety and Support
- The Right to Informed and Conscious Use
- The Right to Digital Literacy

Their report Disrupted Childhood: The Cost of Persuasive Design (July 2018) highlights how persuasive design strategies deployed to maximise the collection of personal data impact on children's social, mental and physical development, and calls for better protections for children and young people.

The 5Rights report Towards an Internet Safety Strategy (January 2019) sets out a framework to prevent harm to children from digital products and services. It sets out seven priorities for the development of online safety strategies: parity of protection, design standards, accountability, enforcement, leadership, education, and evidence-based interventions.

The need for greater online media and digital literacy

9.12 Online media and digital literacy can equip users with the skills they need to spot dangers online, critically appraise information and take steps to keep themselves and others safe online. It can also have wider benefits, including for the functioning of democracy by giving users a better understanding of online content and enabling them to distinguish between facts and opinions online. In recent months, there have been several reports that recognise the importance of online media and digital literacy, calling for action at all levels. Box 37 summarises the recommendations of some of these reports.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Stakeholder calls for action to improve media and digital literacy **Box 37**

- The House of Commons DCMS Select Committee has called for digital literacy to be the fourth pillar of education, alongside reading, writing and maths in its report Disinformation and 'Fake News'. The Committee also noted the role of Ofcom, the ICO, the Electoral Commission and the Advertising Standards Authority in promoting digital literacy, and recommended that the government ensures that the four main regulators produce a more united strategy in relation to digital literacy.
- The Cairncross review, A sustainable future for journalism, published in February 2019,[81] recommended that the government should develop a media literacy strategy, working with Ofcom (which has a statutory duty to promote media literacy), the online platforms, news publishers and broadcasters, voluntary organisations and academics, to identify gaps in provision and opportunities for more collaborative working.
- In 2018, the House of Lords Select Committee on Political Polling and Digital Media stressed the need to teach critical literacy skills in schools to limit the spread of misinformation online and its potential impact on democratic debate.
- The Children's Commissioner's report Growing up Digital, published in 2017, called for the creation of a compulsory digital citizenship programme for pupils aged 4 to 14, to improve children's digital literacy skills and digital resilience and to broaden digital literacy education beyond safety messages.[82]

9.13 There has been significant work in this area, with several organisations in tech, media and civil society developing resources for use in school and at home, to equip children and young people with the skills to critically assess information and keep themselves safe online.

Online safety initiatives: Examples of news literacy initiatives for children and young people* **Box 38**

NewsWise is a free, cross-curricular news literacy project for 9-11 year olds across the UK.

- The project, a partnership between the Guardian Foundation, National Literacy Trust and the PSHE Association, officially launched in September 2018 and Google is funding its first year.
- The project aims to strengthen children's critical thinking skills before they start using social media, and aims to deepen children and young people's understanding of why and how the news is produced, with sessions on selecting facts, checking sources and news analysis to develop children's skills of informed questioning and verification.

81 The Cairncross Review (2019). A sustainable future for journalism. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf

82 Children's Commissioner (2017). Growing up Digital: A report of the Growing Up Digital Taskforce. Available at: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The BBC's Young Reporter project works with young people aged 11-18 in schools, colleges and youth organisations to help them navigate news and current affairs and give them the skills to produce their own reports and share story ideas about what matters to them.

Through the project, all schools have been given access to free online materials including classroom activities, video tutorials and the BBC iReporter game. This interactive game uses the principles of journalism to guide critical thinking by putting the player in the heart of the newsroom on the day of a breaking news story.

9.14 While we welcome these initiatives, we believe that there are notable gaps in provision and that adults need support too – for themselves but also as parents. Ofcom's Children and parents: Media use and attitudes report 2018 (January 2019)[83] notes that parents and carers are increasingly worried about the internet, and are finding controlling screen time harder. Fifty per cent of parents are concerned about the data companies are collecting on children and young people's online activities. They also worry about children damaging their reputations, the pressures of children to spend money and the possibility of children being radicalised online.

9.15 Government is committed to continuing to support parents in preventing and dealing with online harms. Government welcomes the support provided by the UK Safer Internet Centre. They produce a free Safer Internet Day resource pack for parents and carers, most recently in February 2019, helping parents and carers understand the facts about online risks and have positive conversations with their children about staying safe online.

9.16 However, for adults, there is insufficient messaging or resources covering online media literacy. There is a need for further work to address issues such as the sharing of disinformation, catfishing (i.e. luring someone into a relationship by means of a fictional online persona), attacks on women online (particularly public figures), and the differing needs of people with disabilities when navigating information. We also recognise the need for improved coordination of activity. Ofcom is working with a number of partners to assess existing research and evidence about people's attitudes and understanding of being online. This will assist policy-makers to identify gaps and opportunities.

Online safety apps: NewsGuard **Box 39**

NewsGuard was first launched in the US in March 2018 by journalists to tackle the problem of disinformation online and is now available to UK users.

- NewsGuard rates and reviews news and information websites using nine standards of credibility and transparency, allocating a 'nutrition label' review which provides information on the site's ownership, financing, content, credibility, transparency, and history.
- The NewsGuard desktop browser extension displays these 'nutrition labels' next to headlines in social media feeds and search results. This has been rolled out in libraries in the US, and Microsoft now offers the extension as an optional setting in the desktop and mobile versions of its Edge browser.

83 Ofcom (2018). Children and parents: Media use and attitudes report 2018. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

An online media literacy strategy

9.17 Industry and government have a shared responsibility to empower users to manage their online safety. The new regulator will have oversight of industry activity and spend, and a responsibility to promote online media literacy.

9.18 Ahead of the new regulator, the government will develop an online media literacy strategy. The media literacy field is a broad one, and we will therefore consult widely, possibly through a new taskforce, in order to ensure its objectives are well informed by evidence and take account of existing work.

9.19 The first step will be a comprehensive mapping exercise to identify what actions are already underway, and to determine the objectives of an online media literacy strategy. This process will involve convening representatives from tech companies, regulators, libraries, civil society, academics and government to identify ways to strengthen existing provisions, as well as to identify what additional activity is needed to make progress against key objectives, which may include:

- Ensuring that users can be more resilient in dealing with mis- and disinformation, including in relation to democratic processes and representation.
- Equipping people to recognise and deal with a range of deceptive and malicious behaviours online, including catfishing, grooming and extremism.
- Ensuring people with disabilities are not excluded from digital literacy education and support.
- Developing media literacy approaches to tackling violence against women and girls online.

9.20 The strategy will also reflect the government's commitment to look at how to give the public confidence in online information so they are equipped to make their own decisions about the issues that matter. The government has already invested over £1 million in 2018/19 to deliver two initiatives in support of this:

- The new 'RESIST' counter-disinformation toolkit equips government, public service and partner country communicators with the knowledge and skills they need to identify, assess and respond to disinformation. It will help develop a strategic and consistent counter-disinformation capability, and help reduce the impact of disinformation campaigns on UK society and our national interests, in line with our democratic values.
- Government has launched a pilot public disinformation communications campaign.[84] This campaign provides the public with the skills they need to recognise and respond to disinformation, showing people how it can affect them and what they can do about it.

The role of the tech sector in empowering users

9.21 As set out above, we recognise that companies fund a range of valuable education and awareness activities. However, we believe there needs to be greater transparency about the level of investment, that all activity needs to be evaluated to ensure resources are directed at the most impactful initiatives, and that there should be greater coordination across industry to avoid duplication.

84 https://sharechecklist.gov.uk/

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

9.22 The new regulator will have the power to require companies to report on their education and awareness raising activity. We are consulting on appropriate powers for the regulator in this area.

Consultation questions

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Part 5: Conclusion and next steps

10: Conclusion and next steps

10.1 This White Paper sets out the UK's ambitious vision for online safety, including a new regulatory framework to tackle a broad range of harms; the development of a safety by design framework and support for innovation in safety technologies; and a new online media literacy strategy.

10.2 The measures outlined in this White Paper are novel and ambitious, with potentially far reaching effects for how our society engages with the internet. The UK remains committed to a multi-stakeholder model of internet governance as the best way to ensure a free, open and secure internet. All stakeholders from industry, civil society and government have a responsibility to help address legitimate online harms.

10.3 Given this, we want to engage with the widest possible audience on our proposals, and in particular invite views from industry, civil society, think tanks, campaigners and representatives. A series of consultation questions are posed throughout this document and they act as a basis for a formal consultation. We encourage respondents to provide not just their opinions, but also the supporting facts and reasoning to inform the evidence base for the development of our final proposals.

10.4 The consultation begins on 8 April 2019 and will close 12 weeks after it opens on 1 July 2019. We will then publish the government's response to this consultation on the GOV.UK website, summarising the responses received and setting out the action we will take, or have taken, in respect of them in developing our final proposals for legislation. Further information on responding to this consultation can be found in annex A.

10.5 DCMS and the Home Office will also run a series of engagement workshops to convene civil society actors and user groups. This will focus in particular on groups which are disproportionately affected by online harm and abuse. Given the formal and technical nature of the consultation, this will allow us to facilitate engagement with a wider audience.

10.6 Alongside this, we will continue to draw on advice from legal, regulatory, technical, online safety and law enforcement experts, to inform the further development of these proposals.

10.7 Finally, we are committed to continuing to build the evidence base for our proposals and will continue to work across government and with other stakeholders, including UKCIS, to commission a suitable programme of research.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Legislation

10.8 Following the publication of the Government Response to the consultation, we will bring forward legislation when parliamentary time allows.

Note on territorial scope

10.9 Internet services and their regulation is a reserved issue, therefore we intend for our proposed framework to apply on a UK wide basis. While some of the harms in the scope of this White Paper relate to offences in Scots or Northern Ireland Law, and therefore involve devolved competencies (such as child protection), we are not seeking to change the law in relation to these offences but rather to clarify the responsibility of companies to tackle this activity on their services. Education policy is devolved in Wales, Scotland and Northern Ireland.

10.10 As part of the wider process of consultation, we will engage with the Devolved Administrations on the proposals in this White Paper. This consultation will consider in particular the implications for law enforcement, and explore how we can advance a cohesive UK-wide approach to educating children and adults about online safety.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Annex A: How to respond to the consultation

We are inviting individuals and organisations to provide their views by responding to the questions set out throughout this White Paper. The questions are listed below.

The consultation will be open for 12 weeks, from 8 April 2019 to 23:59 1 July 2019.

You can respond online via the following link:
https://dcms.eu.qualtrics.com/jfe/form/SV_5nm7sPoxilSoTg9

If you prefer, you can also email your response to:
onlineharmsconsultation@culture.gov.uk

Or you can write to us at:

Online Harms Team
DCMS
100 Parliament Street
London
SW1A 2BQ

Consultation Questions:

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

> Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Question 6 In developing a definition for private communications, what criteria should be considered?

Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?

> Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

Question 9: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?

> Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?

Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

Question 14: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

> Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?
>
> Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



HM Government

ISBN 978-1-5286-1080-3
CCS0219683420

Pages 397 to / à 401

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Int'l, 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu

CANADIAN CENTRE *for* CHILD PROTECTION®
Helping families. Protecting children.

CHILD SEXUAL ABUSE IMAGES ON THE INTERNET: A Cybertip.ca Analysis

Summary of Key Findings

January 2016

The Canadian Centre for Child Protection Inc. (Canadian Centre) is a charitable organization dedicated to the personal safety of all children. Our goal is to reduce the incidence of missing and sexually exploited children while educating the Canadian public about ways to keep children safe.

The Canadian Centre operates Cybertip.ca, Canada's tipline for reporting the online sexual exploitation of children. Like many other hotlines around the world, Cybertip.ca has seen a marked increase in the volume of reports over the past few years. In 2015, the tipline processed 37,352 reports and it is expected that this will continue to increase in the coming years. This significant rise in reporting is primarily related to the public's concerns involving child sexual abuse images and videos on the Internet (over 95% of reports).

In January 2016, the Canadian Centre released its study *Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis*. This report provides an overview of the information received through reports to the tipline over the last 8 years, with a particular focus on child sexual abuse images. The report was based on the review of close to 152,000 reports and examined 43,762 unique images and videos classified by Cybertip.ca as child pornography.



Child pornography is a recording of a child being sexually exploited or abused. The image or video becomes a permanent record of a child's abuse and can propagate indefinitely. In order to produce the content, a child has to be assaulted or posed deliberately in a sexualized way. In our experience, possessing, distributing and making child sexual abuse content is rarely, if ever, accidental.

cybertip!ca®

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



The harsh reality is that 78.29% of the images and videos analyzed by Cybertip.ca depict very young, pre-pubescent children under 12 years old, with the majority of those being under 8 years of age (63.40%).



As the age of the children decreases, the sexual abuse and sexual exploitation acts become more intrusive. When babies and toddlers were seen in the images and videos, 59.72% of the abuse acts involved explicit sexual activity/assaults and extreme sexual assaults against the child.



The inclusion of a boy child in the image or video increased the likelihood that the content depicted explicit sexual activity/assaults or extreme sexual assaults.

© 2016, Canadian Centre for Child Protection Inc. All rights reserved. Users are granted permission to save and print copies as needed for personal, research and other non-commercial use provided the source of information is attributed to the copyright owner.

"CANADIAN CENTRE for CHILD PROTECTION" and "cybertip!ca" are registered in Canada as trademarks of the Canadian Centre for Child Protection Inc.

The full report can be accessed online at www.protectchildren.ca.

All images depict models and are intended as illustrative.

KEY FINDINGS

Key findings from *Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis* include:

- 78.29% of the images and videos assessed depicted very young, prepubescent children under 12 years old
- 63.40% of those children under 12 years old appeared to be under 8 years of age
- 6.65% of those children under 8 years old appeared to be babies or toddlers
- 80.42% of the children were girls
- 77.05% of the children's faces were visible in the images and videos
- 50.00% of the images and videos involved explicit sexual activity/assaults and extreme sexual assaults
- 53.84% of the abuse acts against children under 12 years old involved explicit sexual activity/assaults and extreme sexual assaults
- 59.72% of the abuse acts against babies and toddlers involved explicit sexual activity/assaults and extreme sexual assaults
- 68.68% of the images and videos appeared to be in a home setting, of which 69.91% captured explicit sexual activity/assaults and extreme sexual assaults
- 83.35% of the adults visible in the images and videos were males
- 97.25% of the content involved explicit sexual activity/assaults and extreme sexual assaults when adult males were visible with the children in the images and videos

RECOMMENDATIONS

Through our role in operating Cybertip.ca over the past 13 years, our organization has witnessed the growing proliferation of child sexual abuse images and videos on the Internet. We know that more needs to be done to identify and support child victims of sexual abuse, identify and prosecute offenders, and reduce the availability of child sexual abuse material on the Internet. The following are some of the Canadian Centre's recommendations for strengthening our commitment to fight the exploitation and sexual abuse of children:

- Identify and rescue more victims in child sexual abuse material by working closely with child exploitation units, and improve support services in Canada to better protect the rights of victims when abuse material is circulating online.
- Reduce the availability of child sexual abuse material to Canadians by leveraging technology to disrupt the growing problem of sexual abuse material online, strengthening private sector involvement, and strengthening Canada's role internationally.
- Increase reporting by Canadians through national public awareness campaigns and working with relevant stakeholders to promote reporting.
- Stop offenders by enhancing resources and training in Canada including increased police and forensic capacity, adopting best practices related to reducing online sexual exploitation of children and adapting the *Criminal Code* and related legislation to aid in the tackling of this problem.
- Focus efforts on prevention and education using recognized prevention programming in addition to the creation of new resources for parents, health care professionals, and public facilities (e.g., pools).

"Unlike other forms of exploitation, this one is never ending. [Every day,] people are trading and sharing videos of me as a little girl being raped in the most sadistic ways... They are being entertained by my shame and pain."

Excerpt from Victim Impact Statement filed by a now adult victim of child pornography, quoted in United States of America v. Lindauer, Case No. 3:10-cr-00073, US District Court for the Western District of Virginia

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Canadian Centre for Child Protection (CP3) 2016

International Survivors' Survey

To better understand the unique challenges faced by survivors, the Canadian Centre launched the International Survivors' Survey in January 2016. Over the course of a year and a half, 150 survivors from around the world completed the comprehensive survey, contributing valuable details and information about their experience.

We recognize how incredibly difficult and challenging it may have been to complete the survey and we deeply appreciate that so many survivors took the time to share their story with us.

I had to smile nicely and pretend I liked it just like those women in the movies because that was what the men who would get it wanted to see.... I just had to deliver what was asked from me. And that was the reason I quite soon understood it was meant for other people.

- Survivor in response to the question, "What were the circumstances in which the offender said they would show someone else the imagery?

International Survivors' Survey Results

In September 2017, the Canadian Centre released results from the International Survivors' Survey for now-adult survivors whose child sexual abuse was recorded and/or distributed online, with recommendations to address this horrific crime. Some of the results include:

- Almost 70% of the survivors worried about being recognized by someone because of the recording of their child sexual abuse. In fact, **30**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

respondents reported being identified by a person who had seen their child sexual abuse imagery.

- 58% of respondents reported having had more than one person abusing them, while 82% of the primary offenders involved in multiple offender scenarios were **parents or extended family members of the child.**
- 56% of the survivors indicated that **the abuse began before the age of four**, and 87% were 11 years of age or younger. 42% were abused for more than 10 years.
- At least 74 respondents (nearly 50%) were survivors of **organized sexual abuse**(abuse that involves children being subjected to sexual abuse by multiple offenders).
- 67% of the survivors were **threatened with physical harm** including being told they would die or be killed.
- 85% of the survivors anticipated needing **ongoing/future therapy**.

I remember being humiliated when my abuser showed another child (whom I liked) photos of my torture (with ropes). I wanted to hide these images because of the shame, so disclosure would have been nearly impossible. Disclosure would implicate me in what I believed was a crime for which I was at least partially responsible.

❖ Survivor in response to the question, "Please describe how the existence of images of your abuse impacted your decision to tell someone (if at all)."

Recommendations for Change

The survey results underscore the urgent need for the international community to take immediate action and implement the following recommendations:

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Reduce the availability of both new and existing child sexual abuse images and videos on the public internet. Consideration should be given to adopting Project Arachnid as the global platform for quickly detecting the presence of child sexual abuse material online and issuing takedown requests to hosting providers, notifying them of the presence of the content on their service and requesting immediate removal of the material.

Improve education and training on the issue of child sexual abuse among professionals to empower them to recognize and respond appropriately. Those in a position to uncover abuse must better understand the dynamics of different abuse situations, the complex process of disclosure, and the role of technology in facilitating child sexual abuse.

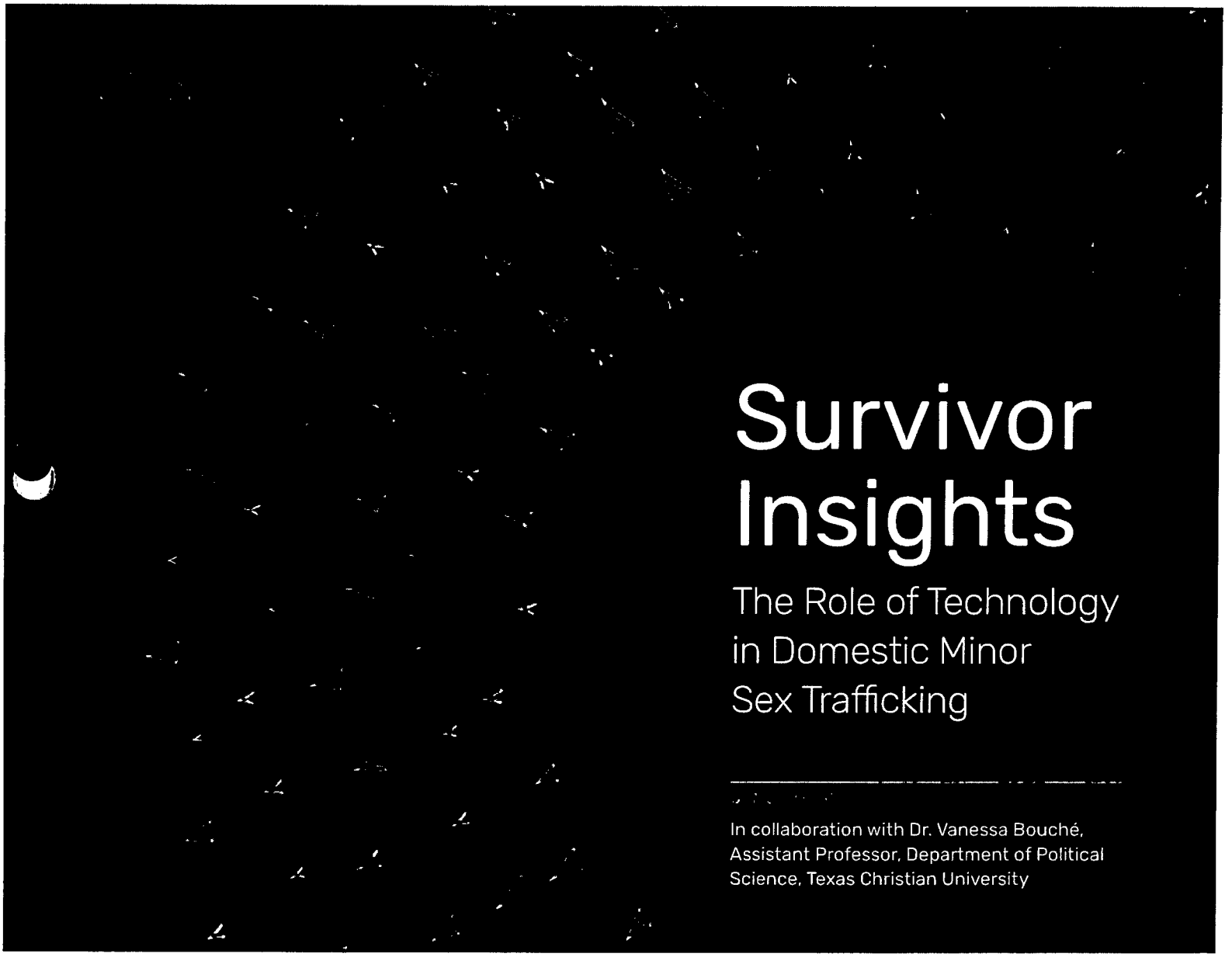
Strengthen the coordination and communication between all systems and entities that intersect with victims of child sexual abuse and online exploitation. This includes, but is not limited to, child welfare, schools, hotlines, therapists, police, industry, child-serving organizations, and advocacy centres.

Develop comprehensive systems and remedies to properly recognize the rights and unique needs of victims whose abuse was recorded. This includes accessible, knowledgeable therapists and attainable mechanisms for receiving financial compensation. Survivors must also be provided with the opportunity to have their voices heard within the criminal justice system (e.g., victim impact statements).

[The survey] was very good for me. It allowed me to actually tell people what I felt with no real barriers. It also gave me a sense of empowerment over some of what happened.

- Survivor

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Survivor Insights

The Role of Technology in Domestic Minor Sex Trafficking

In collaboration with Dr. Vanessa Bouché, Assistant Professor, Department of Political Science, Texas Christian University

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Executive Summary

I felt like a slave working for someone, getting beat and not getting paid, not having control over my own life.

– Survey Respondent

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

STAT HIGHLIGHTS

260
Survivors of DMST

1 in 6
Trafficked under the age of twelve

75%
Of those who entered the life in 2004 or later were advertised online

In an effort to strategically inform technology initiatives for combating domestic minor sex trafficking (DMST), Thorn partnered with Dr. Vanessa Bouché at Texas Christian University to survey survivors about their experiences. The survey focused on understanding what role technology played in a victim's recruitment into, time while in, and exit from DMST.

Two hundred and sixty survivors of DMST, through 24 survivor organizations, spanning 14 states, completed the survey.

The majority of participants identified as female (98%), 2% as male, and 1% as "other".[1] Sixty-seven percent identified as heterosexual, 25% bisexual, 5% homosexual, 2% "other", and 1% "don't know". Among those identifying race (n=243), 45% reported African American, 27% Caucasian, 21% Hispanic, and 8% "other".

Two central themes emerged from survey responses:

1 **Technology is playing an increasing role in grooming and controlling victims of DMST.**

2 **Less familiar forms of DMST, including those trafficked by family members or without a clear trafficker, emerged in the DMST landscape. However, consistent in all types of DMST observed are common experiences of childhood abuse and neglect.**

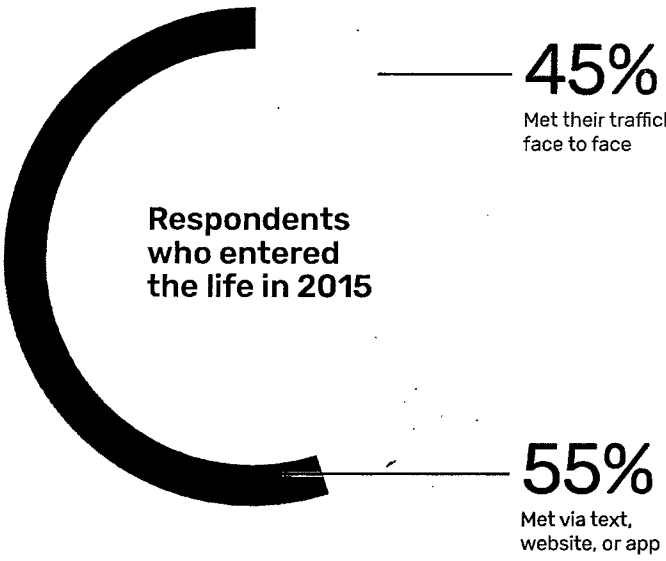
These themes suggest an important understanding about the nature of DMST and the role of technology. The need for human connection, and the vulnerabilities that arise in the absence thereof, are central to the recruitment, control, and recovery of DMST survivors. Use of technology is likely to continue to increase; however, technology is unlikely to extinguish the human element of DMST.

[1] Does not total to 100% due to rounding.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Role of technology is increasing

Not surprisingly, use of technology by traffickers, victims, and buyers is increasing. The Internet and cellular technology offer individuals the opportunity to stay connected around the clock and from any distance, and it offers access - to information, goods, and people - that previously was out of reach. These same benefits support its growing popularity in DMST.



RECRUITMENT AND GROOMING. Across the sample, most traffickers continue to meet and groom victims through face to face contact. However, respondents who entered the life in 2015 noted much higher uses of technology in this process. Across the sample, 84% reported meeting their trafficker for the first time face to face, but only 45% of those entering the life in 2015 reported meeting their trafficker face to face. The remaining 55% reported use of text, website, or app. Similarly, 85% of the entire sample reported their trafficker spent time with them in person to build a relationship. By comparison, only 58% of those who entered the life in 2015 reported time in person as the means for building a relationship. Of those whose trafficker used technology in this process, 63% reported communicating online and 25% reported communicating via phone call.

Importantly, 2015 data deviated from the rest of the sample; therefore, continued investigation into the use of technology in meeting and grooming victims is required. However, the findings do show that while meeting in person was the singular dominant method of developing a close relationship in the past, it is now a dominant method while technology-based modes of communicating are increasing in usage.

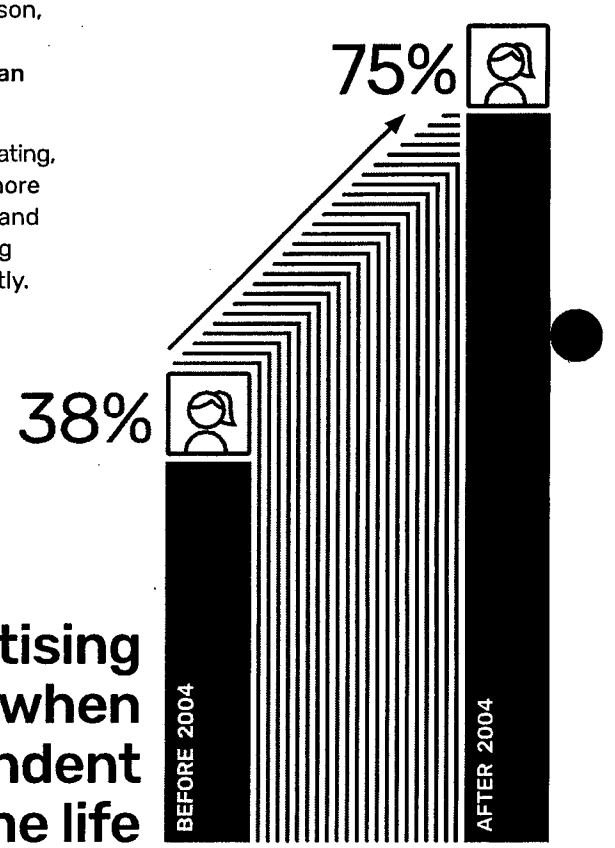
Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

EXPERIENCE IN THE LIFE. While in the life, most victims do have access to the Internet and 90% of those report using social media. Victims are using social media to communicate with family, friends, traffickers, and buyers. Interestingly, findings suggest **monitoring of both Internet and cell phone use is decreasing.** The most popular websites accessed by victims were Facebook, Backpage, Craigslist, Instagram, and Google.

Online advertising is increasing while advertising on the street is decreasing. Prior to 2004, the predominant forum for advertising was on the street (78%) and only 38% were advertised online. By comparison, **for those who entered the life in or after 2004, street advertising had dropped to 61% and online advertising had increased to 75%.** The most frequently reported platform for online advertising was Backpage. The next most popular sites included Craigslist, RedBook, SugarDaddy, and Facebook.

Online advertising was also associated with an increased number of buyers per day. One in seven respondents who were advertised on the street reported more than 10 buyers per day. By comparison, one in four respondents who were advertised online reported **more than 10 buyers per day.**

By using remote means of communicating, traffickers are able to engage with more victims and buyers simultaneously and around the clock, thereby expanding their reach and influence significantly.



Online advertising based on when respondent entered the life

THORN

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

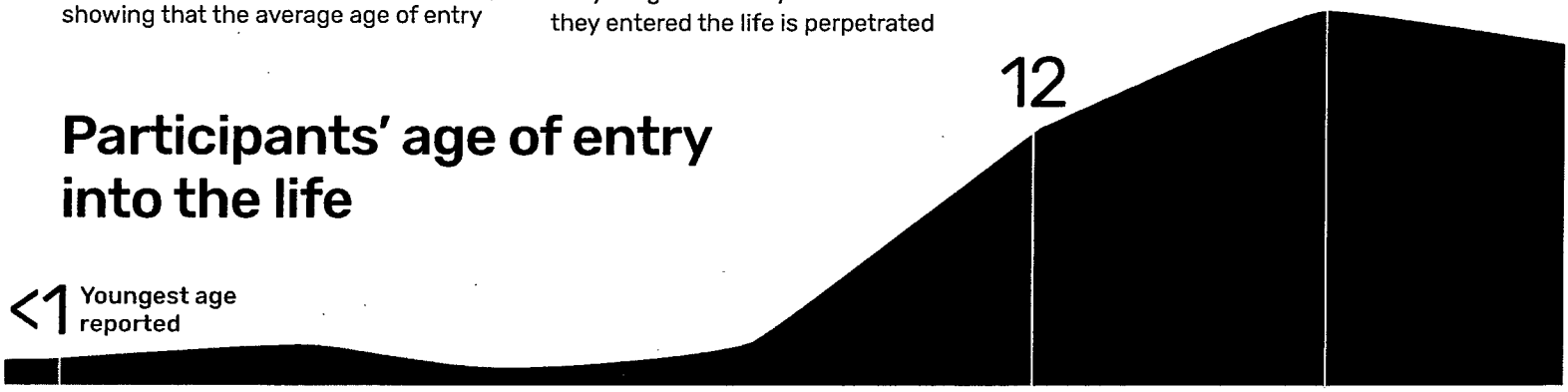
Less familiar trafficking experiences and shared vulnerabilities

Survey responses underscored numerous social factors that influenced respondents' experiences while in the life, and later on their road to recovery. Adverse childhood experiences increased vulnerability of exploitation. Recurring victimization by those in positions of trust bred distorted views of self-worth, love, and security.

The survey found that the median age entering the life was 14 years old. This corroborates other research on DMST showing that the average age of entry into commercial sexual exploitation is roughly 12 to 14 years old. While **the most frequently reported age of entry into the life was 15, one in six participants reported being trafficked before the age of 12 with the youngest victims less than 1 year old.**

Respondents described a range of trafficking experiences in the life including the following general categories: familial, non-familial, or no trafficker. The survey found that in some cases children may be born into sex trafficking, or be forced into it as a toddler. Sex trafficking of those that are younger than 10 years old when they entered the life is perpetrated almost exclusively by family members, often a father or stepfather. This early entrapment in the life colored their understanding of individual value or purpose with one respondent stating it was explained to them as *"what all little girls and boys do for their parents"*. Another underscored that being trafficked by a family member made escape seem impossible, stating *"I could never escape. I never have anyone to turn to. I didn't have a choice. I was born into this."*

Participants' age of entry into the life



ONE IN SIX WERE UNDER THE AGE OF 12

THORN

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Respondents who entered the life after age 11, were most likely to be trafficked by strangers, followed by people in their social network. In some cases, respondents reported a trafficker's offer of food and shelter was their first step into the life. In other cases, a trafficker's promise of love and wealth helped to earned their trust.

Even among those that were not trafficked by their own family, the survey results reveal that many DMST victims experienced some form of childhood abuse and neglect, reporting high rates of verbal, physical, or sexual abuse. Given these adverse childhood experiences, two out of three participants had experiences with either foster care or juvenile detention. These environments likely increased exposure to negative influences including traffickers or other victims of DMST that used their access to recruit new victims.

Throughout the report there are some significant differences between those who had a trafficker while in the life and those who reported that they did not. Nineteen percent of participants reported that they did not have a trafficker. It is likely a trafficker existed in some of these cases, but was not recognized as such by the respondent. Analysis of responses found that 42% of these respondents were subject to physical and psychological coercion by someone in relation to DMST. Others reported engaging in survival sex for access to food, drugs, or other needs.

Those reporting no trafficker appeared to have significantly more freedom, evidenced by having fewer buyers per day, being able to use their phones more frequently, having unmonitored Internet access, advertising less, and being less likely to say that they wanted help exiting the life.

Even after exiting the life, many do not characterize themselves as victims and may continue to romanticize their relationship with the trafficker. **Less than one quarter have seen their trafficker prosecuted and when asked if they would want to pursue prosecution of their trafficker, a strong majority (88%) reported they would not.**

Recommendations

Findings of the survey support many initiatives currently underway to combat DMST such as supporting stable and loving homes, increasing awareness in the community, and expanding available support resources such as shelters and job training. These efforts play an important role in protecting vulnerable children and identifying traffickers, and should be sustained and grown when possible. In addition, survey responses suggest several opportunities for improved prevention, intervention, and recovery.

Prevention programs must be aimed directly at children and youth, and therefore require

"It's easy to get in and hard to get out."

– Survey Respondent

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

examining those places where children and youth – especially the highest risk – are likely to be. Survey responses indicate most children were in school while in the life, and most had experiences with the foster care or juvenile detention systems at some point. **Schools were also noted by survivors as a key opportunity for intervention** noting, *"A teacher would have been the most helpful to either give me the number [of the helpline] or call for me."*

"A teacher would have been the most helpful to either give me the number [of the helpline] or call for me."

Given the increasing use of technology for grooming victims and advertising to buyers, tech companies are uniquely positioned to combat DMST and engage with victims. For example, findings suggest increasing use of social media and apps by buyers to communicate with traffickers and victims. Further examination of patterns in this process could help industry identify bad actors on their platforms. Tech companies could also deliver online help advertisements via platforms frequented by victims. For example, most respondents reported they never saw a helpline number while in the life, and those that did not see the helpline number encouraged use of social media for placement. Improving visibility of resources such as helplines on platforms known to be frequented by DMST victims could increase opportunities for exiting the life.

Findings also indicate there may be investigative value in how a trafficker communicates with buyers. Younger victims with traffickers were significantly more likely to report the trafficker communicated directly with buyers (rather than the victim communicating with buyers). As such, factoring in who is communicating with buyers may facilitate investigative risk assessments and victim identification.

Respondents underscored the continued need for increased availability of support services when exiting the life, with particular attention on counseling services. For many, they are in areas with limited access to trauma-informed counseling services that meet their needs as survivors of DMST. One participant suggested that the creation of virtual counseling communities could fill this need.

Finally, acknowledging the quickly shifting landscape in any area involving technology, it is important to continuously review how technology is used by traffickers, victims, and buyers. Thorn plans to continue its efforts on this front and is reviewing methods for ongoing monitoring of technology trends in DMST.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Closing Remarks

The stories shared by DMST survivors about their experiences offer critical insights into the world of DMST and must be included in any strategy to combat DMST. The 2016 Survivor Survey not only suggests traffickers are increasingly using technology to ensnare victims in the life and advertise minors for sex, it also highlights opportunities to use technology to protect those targeted by traffickers. However, technology alone will not be sufficient. While promising technological interventions can play a vital role in engaging victims and identifying traffickers, we cannot ignore the human element of trafficking. We must continue to address those abuses that make children vulnerable and empower them on their road to recovery.

THORN

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

This report was made in collaboration with Dr. Vanessa Bouche, Assistant Professor of Political Science at Texas Christian University. Dr. Bouché is currently a co-principal investigator on three federally-funded grants on human trafficking, two from the National Institute of Justice and one from the United States Agency on International Development. Her research has been published in the Journal of Politics, Journal of Public Policy, Politics & Gender, among other outlets.

THANK YOU

Without the dedication of the following individuals, this work wouldn't have been possible: Leah Treitman, Melissa Stroebel, Brooke Istook, Kristy Kosak, and Sarah Potts.

Designed by Kelsey Lesko

THANK YOU

We would like to thank the following direct service organizations for their gracious participation. Without their hard work, this report would be nothing more than a wish:

Breaking Free

Coalition to Abolish Slavery & Trafficking

Phoenix Dream Center

Rebecca Bender Initiative

Safe Harbor/Center for Youth Services

The Hope Project

The Link-Passageways

Traffick911

Pages 418 to / à 420

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Subv, 15(1)(d)(ii), 16(1)(a)(iii), 16(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Standing Against Hate

Facebook blog post announcing a ban on praise, support and representation of white nationalism and white separatism

Facebook Newsroom | March 27, 2019

Today we're announcing a ban on praise, support and representation of white nationalism and white separatism on Facebook and Instagram, which we'll start enforcing next week. It's clear that these concepts are deeply linked to organized hate groups and have no place on our services.

Our policies have long prohibited hateful treatment of people based on characteristics such as race, ethnicity or religion — and that has always included white supremacy. We didn't originally apply the same rationale to expressions of white nationalism and white separatism because we were thinking about broader concepts of nationalism and separatism — things like American pride and Basque separatism, which are an important part of people's identity.

But over the past three months our conversations with members of civil society and academics who are experts in race relations around the world have confirmed that white nationalism and white separatism cannot be meaningfully separated from white supremacy and organized hate groups. Our own review of hate figures and organizations – as defined by our Dangerous Individuals & Organizations policy – further revealed the overlap between white nationalism and white separatism and white supremacy. Going forward, while people will still be able to demonstrate pride in their ethnic heritage, we will not tolerate praise or support for white nationalism and white separatism.

We also need to get better and faster at finding and removing hate from our platforms. Over the past few years we have improved our ability to use machine learning and artificial intelligence to find material from terrorist groups. Last fall, we started using similar tools to extend our efforts to a range of hate groups globally, including white supremacists. We're making progress, but we know we have a lot more work to do.

Our efforts to combat hate don't stop here. As part of today's announcement, we'll also start connecting people who search for terms associated with white supremacy to resources focused on helping people leave behind hate groups. People searching for these terms will be directed to Life After Hate, an organization founded by former violent extremists that provides crisis intervention, education, support groups and outreach.

Unfortunately, there will always be people who try to game our systems to spread hate. Our challenge is to stay ahead by continuing to improve our technologies, evolve our policies and

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

work with experts who can bolster our own efforts. We are deeply committed and will share updates as this process moves forward.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

YouTube's Product Chief on Online Radicalization and Algorithmic Rabbit Holes

Neal Mohan discusses the streaming site's recommendation engine, which has become a growing liability amid accusations that it steers users to increasingly extreme content.

By Kevin Rose | The New York Times | March 29, 2019

It's been called "one of the most powerful radicalizing instruments of the 21st century," "a petri dish of divisive, conspiratorial and sometimes hateful content," and a tool that "drives people to the internet's darkest corners."

I'm talking, of course, about YouTube — and, specifically, the recommendation algorithm that determines which videos the site plays after the one you're watching. That algorithm is YouTube's beating heart, keeping users hooked to the platform for hours on end. (The company has said recommendations are responsible for about 70 percent of the total time users spend on the site.)

The recommendation engine is also a growing liability for YouTube, which has been accused of steering users toward increasingly extreme content. After the recent mass shooting in Christchurch, New Zealand — the work of a gunman who showed signs of having been radicalized online — critics asked whether YouTube and other platforms were not just allowing hateful and violent content to exist but actively promoting it to their users. YouTube's biggest competitor, Facebook, said last week that it would ban white nationalism and white separatism on its platforms.

I recently spoke with Neal Mohan, YouTube's chief product officer, about criticism of the company's algorithms and what it is doing to address radicalization and violent extremism on the platform. We spoke about the things YouTube has already done to rein in extreme content — hiring additional reviewers, introducing a "breaking news shelf" that kicks in after major news events, altering the recommendation algorithm to reduce the distribution of conspiracy theories and other "borderline content" — and about the company's plans for the future.

The conversation was edited for length and clarity.

I'm wondering what you think about the conversation happening around radicalization on YouTube.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

I think some of it has to do with the fact that, as you know and as you've written about, YouTube was started as, and remains, an open platform for content and voices and opinions and thoughts. Many of them being, you know, really across the entire spectrum, many of which you or I or others may or may not agree with. I wouldn't be at YouTube, working on what I work on, if I didn't believe in the power of diversity of voices and opinions.

Having said that, we do take this notion of dissemination of harmful misinformation, hate-filled content, content that in some cases is inciting violence, extremely seriously.

I hear a lot about the "rabbit hole" effect, where you start watching one video and you get nudged with recommendations toward a slightly more sort of extreme video, and so on, and all of a sudden you're watching something really extreme. Is that a real phenomenon?

Yeah, so I've heard this before, and I think that there are some myths that go into that description that I think it would be useful for me to debunk.

The first is this notion that it's somehow in our interests for the recommendations to shift people in this direction because it boosts watch time or what have you. I can say categorically that's not the way that our recommendation systems are designed. Watch time is one signal that they use, but they use a number of other engagement and satisfaction signals from the user. It is not the case that "extreme" content drives a higher version of engagement or watch time than content of other types.

I can also say that it's not in our business interest to promote any of this sort of content. It's not something that has a disproportionate effect in terms of watch time. Just as importantly, the watch time that it does generate doesn't monetize, because advertisers many times don't want to be associated with this sort of content.

And so the idea that it has anything to do with our business interests, I think it's just purely a myth.

So, why do people talk about this rabbit hole effect — you know, I went to watch one video about President Trump and now I'm just getting a stream of recommendations of increasingly more partisan content. Why do you think there's this perception that this is what happens on YouTube?

This is one of the things that we looked at closely as we were developing the technology that went into that recommendation change that I described to you from a few weeks back.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

We really looked at this to see what was happening on those "watch next" panels, in terms of the videos that were being recommended. And the first thing that I should say is that when we make recommendations after a video has been consumed, we don't take into account any notion of whether that's less or more extreme.

So when we looked at the data, we saw that a lot of the videos that were being recommended, as you would expect, had to do with the context of the video that was being consumed. That's obviously no surprise, but the videos that you saw on the panel, there were videos that you might consider to be maybe a little bit more extreme than what you had just consumed.

But you'll also see videos that were less extreme, or that you could call more toward the quote-unquote mainstream. It's equally — depending on a user's behavior — likely that you could have started on a more extreme video and actually moved in the other direction.

That's what our research showed when we were looking at this more closely. Now, that doesn't mean that we don't want to address what we talked about, which is just —

Sorry, can I just interrupt you there for a second? Just let me be clear: You're saying that there is no rabbit hole effect on YouTube?

What I'm saying is that when a video is watched, you will see a number of videos that are then recommended. Some of those videos might have the perception of skewing in one direction or, you know, call it more extreme. There are other videos that skew in the opposite direction. And again, our systems are not doing this, because that's not a signal that feeds into the recommendations. That's just the observation that you see in the panel.

I'm not saying that a user couldn't click on one of those videos that are quote-unquote more extreme, consume that and then get another set of recommendations and sort of keep moving in one path or the other. All I'm saying is that it's not inevitable.

In the case of breaking news, you guys made a decision that showing authoritative information to people who were looking for it was important enough to radically shift the way recommendations and search results work, by moving to an approved or "authoritative sources" model rather than using the regular recommendation algorithm. Why not do that for everything?

Let me say a few things about that. The first is that using a combination of those tools of authoritative content and promoting authoritative content is something that can apply to other information verticals, not just breaking news.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Having said that, as you continue to broaden the application of something like that, it's quite a blunt hammer. And so it does come with trade-offs. For example, how do you define something authoritative across the broad swath of YouTube when many of the use cases, as you know, are outside of the information-seeking realm? They're entertainment, they're oftentimes driven by people's personal tastes, like music and comedy and the like.

Right, but you could do it just for politics, hypothetically, and say that for any political video, we're going to move to this "authoritative sources" model.

I think that even when you go to something that broad, it comes with real trade-offs. And I'm just raising the fact that there are considerations there, which is that you are then limiting political discourse to a set of preordained voices and outlets and publications. And I think that especially when it comes to something as charged and societally impactful as politics, there needs to be room for new voices to be heard.

Since the New Zealand shooting, we've heard this question about "Well, the platforms worked together to take down ISIS content. Why haven't they done the same for white supremacy or violent right-wing extremism?" What's the answer there?

The first thing that I would say, just as a matter of fact, is that there were two sets of challenges when it came to the New Zealand shooting. One was everything that we just talked about in terms of surfacing authoritative, high-quality information — not showing, you know, conspiracies or harmful misinformation. That was one bucket.

The other bucket had to do with the velocity at which re-uploads were coming to these various platforms, and that is an area where we collaborated. We worked closely with other platforms in terms of making sure we had fingerprints of these videos, just like they did, and we shared those.

The other thing I would say, just more generally, in the case of violent extremism and limiting those videos on the platform, the reason it's different than what we're talking about here is that those [ISIS] videos took on a particular form. They were often designed for propaganda purposes and recruitment purposes. So they had things like branding and logos, both visually and in terms of the music they might use. Those formed a set of finite clues we could use to bring that content down. And, of course, we collaborated with other platforms to do that.

So much of what YouTube has become over the years is this kind of alternative form of media. People don't go to YouTube because they want the same stuff

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

they would see on TV. They go because they've built relationships with creators that they trust, and when Logan Paul puts out a flat-earth documentary or Shane Dawson questions whether 9/11 happened, there's a sense that YouTube is the place where these "real" explanations are being offered, and maybe that makes this all very hard to undo.

There's nearly two billion people that come to our platform every month. Every one of them is coming for some unique reason, whether it's the latest and greatest music video or a YouTube original, or their favorite creators.

I think when people come to YouTube looking for information, it has resulted in a shift in the way that we think about the responsibility of our platform. As a result of that shift, our product teams here are thinking of all of these solutions, many of which we've talked about here, as a means of addressing that responsibility for making sure that when users are looking for information, YouTube is putting its best foot forward in terms of serving that information to them. But YouTube is also still keeping users in power, in terms of their intent and the information that they're looking for.

It's an ongoing effort. I think we've made great strides here. But clearly there's more work to be done.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

How the Christchurch shooter used memes to spread hate

Learning from years of online right-wing extremism, the shooter made his manifesto a weaponized shitpost.

By Aja Ramona | Vox | March 16, 2019

The man who allegedly shot and killed 49 people at two mosques in Christchurch, New Zealand, framed the attack as a real-life escalation of meme-based internet culture.

Police are currently investigating a sprawling 74-page manifesto that the 28-year-old suspect allegedly wrote and posted on social media shortly before the attack. The document rails against Muslims and immigrants and includes several references to memes and video games.

The shooter posted the manifesto, along with a link to the forthcoming live stream of the promised attack, on 8chan, one of the main online homes of meme-loving right-wing extremists. In the post, he wrote that it was "time to stop shitposting and time to make a real life effort" — meaning, essentially, that it was time to stop fooling around on the internet and turn his extremist views into real-world action.

Then, right before the starting the attack — which he live-streamed to Facebook as if it were a first-person shooter video game — the shooter referenced the "subscribe to PewDiePie" meme. The guns used in the attack were also decorated with memes, mostly insider white nationalist references.

The shooter appears to have been very familiar with extremist corners of the internet. The choices he made — to post a manifesto to a known radical community, and to carry out the attack as if he were doing it "for the lulz" — are unlikely to have been made at random.

Instead, they were most likely designed to entertain his fellow extremists and, above all, to help them see him as someone to admire and even copy. The memetic elements of the manifesto were also most likely designed to provoke the media and the public into sharing it and debating the shooter's actions — thereby increasing the attention, virality, and public debate surrounding the attack, and further spreading the manifesto within the mainstream.

All of this is important to understand, not only to keep public attention focused on the shooter's unthinkable actions instead of memes but because using memes to normalize unconscionable beliefs and behavior has become an established messaging tool for the far right.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Memes within the manifesto serve to draw attention and pique readers' curiosity

The shooter's manifesto, titled "The Great Replacement," repeats false propaganda about immigrants as "invaders" and references a number of radicalizing ideological influences. It also follows a standard method for spreading extremist ideology online, by framing its hateful rhetoric as a joke in an attempt to normalize it and make it appear more acceptable.

It mixes references to memes, shitposts — an internet term for pointless posts intended to derail or distract readers, the baffling nature of which can often approach Dadaist nonsense art — and other bits of benign internet culture with serious ideological dogma. For instance, it randomly includes a well-known piece of copypasta (large blocks of text that get passed around in meme form), for what appears to be satire's sake.

Journalist Robert Evans wrote a blog post shortly after the shooting in which he convincingly argues that the entire manifesto is an example of what it's imitating — that is, it's a giant shitpost meant to simultaneously draw attention to and distract from the white nationalist rationale that motivated the shooter.

"The entire manifesto is dotted, liberally, with references to memes and Internet in-jokes that only the extremely online would get," Evans notes. "They are meant to distract attention from his more honest points, and to draw the attention of his real intended audience." In other words, the shooter wanted to keep the general public guessing about which parts of the manifesto are serious, while he catered to and essentially directly addressed his core audience of fellow white supremacists.

How does this work? There are three main parts to this process, and they each function toward obscuring reality with the intention of spreading the extremist rhetoric contained within.

Using memes to trick people into dismissing a message as "just a joke" and not serious.

Relying on members of the public to spend time dissecting, responding to, and being distracted by the memetic format of the message.

Concealing the "actual" message within the "joke" of the meme, so that it spreads in all seriousness while the meme gets amplified and discussed.

One of the most significant and pernicious ways that right-wing extremists use trolling, shitposting, and memes is to distort what their actual message is, so they can claim plausible deniability that their message is harmful or bad. That way, even when their extremism is clearly

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

shown to be sincere, the irony surrounding the message clouds the truth. The shooter's manifesto is a textbook example of this.

And to break down why, we have to briefly pay as much attention to the memes, and the artifice around them, as we do to the abhorrent racism they're meant to spread.

The manifesto's meme use is strategically designed to obfuscate its racism

Consider that copypasta I mentioned above. It appears in the middle of a lengthy "FAQ" section in the manifesto:

> **You are a bigot,racist,xenophobe,islamophobe,nazi,fascist!**
>
> A. Compliments will get you no where.
>
> B. That isn't a question.
>
> C. What the fuck did you just fucking say about me, you little bitch? I'll have you know I graduated top of my class in the Navy Seals, and I've been involved in numerous secret raids on Al-Quaeda, and I have over 300 confirmed kills. I am trained in gorilla warfare and I'm the top sniper in the entire US armed forces. You are nothing to me but just another target. I will wipe you the fuck out with precision the likes of which has never been seen before on this Earth, mark my fucking words. You think you can get away with saying that shit to me over the Internet? Think again, fucker. As we speak I am contacting my secret network of spies across the USA and your IP is being traced right now so you better prepare for the storm, maggot. The storm that wipes out the pathetic little thing you call your life. You're fucking dead, kid. I can be anywhere, anytime, and I can kill you in over seven hundred ways, and that's just with my bare hands. Not only am I extensively trained in unarmed combat, but I have access to the entire arsenal of the United States Marine Corps and I will use it to its full extent to wipe your miserable ass off the face of the continent, you little shit. If only you could have known what unholy retribution your little "clever" comment was about to bring down upon you, maybe you would have held your fucking tongue. But you couldn't, you didn't, and now you're paying the price, you goddamn idiot. I will shit fury all over you and you will drown in it. You're fucking dead, kiddo.

This is "the Navy Seal" meme, a well-known shitpost in which an internet forum user rants in exaggerated, overblown fashion. It's been around online for years, but it still frequently gets taken seriously when it's used.

Many memes don't always register as memes, especially as they spread further from their point of origin — so the way people respond to them becomes a barometer for how internet-savvy and knowledgeable they are about internet culture.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

As a bonus, if you recognize a meme when someone else doesn't, you get to feel superior to that other person. So the inclusion of the Navy Seal meme in the manifesto simultaneously becomes about wink-wink-nodding to anyone who gets it, while jarring and discombobulating people who don't.

In the context of the larger manifesto, it's a giant distraction, because anyone who doesn't recognize it has to waste time sorting out what's true and what's false — some early media reports were duped into reporting that the shooter had military experience. Plus, the overall amount of time spent identifying and explaining the memes detracts from the time we could be using to trace the shooter's extremist views back to their roots, as well as to their counterparts in global politics.

Meanwhile, the average person reading the document might be drawn to the copypasta, the giant wall of shouty text, and become distracted by the question of whether that text is sincere or legitimate — distracted from the fact that it comes in an "FAQ" section immediately after the shooter has written, "You are a bigot,racist,xenophobe,islamophobe,nazi,fascist" [sic] about himself.

The manifesto does express the views of a bigoted, racist Islamophobe who states his abhorrent white nationalist views throughout the document in great detail. A primary goal of including the meme seems to be to make the public focus less on that fact, and more on the novelty of the memes, thereby ensuring that the manifesto draws attention.

But the ultimate goal of including the memes seems to be a show of solidarity with the manifesto's primary audience: the "insiders" who understand that while the copypasta is a joke, nothing about the extremist ideology is. The memes inserted into the manifesto serve to bolster fellow extremists' enthusiasm, making them feel even more unified as people who "get" the references and subscribe to the racist views. Ultimately, the memes help turn the manifesto itself into a radicalizing force.

The manifesto is a textbook example of the way right-wing extremists manipulate the media and internet culture

The manifesto also, in classic shitpost form, anticipates the mass media and public's reaction: that is, the entire document is intended to be a signal to the true audience, to the people who "get it," while confusing and distracting those who don't.

It is intended to predict and spoof how the writer expects progressives and members of the media will react — with shock, outrage, and confusion over the various distractions placed in their path, which in this case are the memes themselves.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

And, as the existence of this very explainer proves, it is correct in its prediction. Journalists — who are ethically obligated to not spread misinformation — must dispel the parts of the manifesto that are meant to confuse the public, like the Navy Seal meme. But that also serves to distract from its real message of hate.

It may not be intuitive to discuss how trying to demystify memetic messages instead works to amplify them, but that's precisely what couching the manifesto in memes allows it to do. That is also why the alt-right has strategically and openly been using memes to spread its ideology for years.

In December 2018, I spoke to Whitney Phillips, a well-known expert in online trolling and media literacy, about the rise of online extremism on YouTube. We discussed several issues that Phillips had written about recently, in a guide to help journalists avoid spreading toxic ideologies while reporting on them.

Phillips explained to me how journalists and other members of the public frequently fall into the same kind of trap that the New Zealand shooter's alleged manifesto set.

"A lot of journalists have a kind of perspective that the only way to deal with the pervasive real problems on the internet is if we call attention to them, so that we can begin to kind of uncouple negative influence or hate speech," she said. "Light disinfects — that's the adage."

She went on to explain that a lot of times, that approach is exactly right: "For a certain subset of the audience, light does disinfect. That's absolutely the appropriate tack you should take: that you explain what's happening, and that once those audience members have that information, then they can go forward and be better-informed citizens. Right? Participating in a democracy."

However, she also warned of the dangers of writing extensively about topics that are used to spread extremist ideology: "But that doesn't account for all the other audience members for whom light doesn't just not disinfect, it only serves to illuminate. And in the case of conspiracy theorizing, even if you are fact-checking or trying to debunk, in order to, you know, shed light on a particular problem, or to just make it clear that this one thing that people thought happened didn't actually happen — by doing that, in this weird, upside-down kind of way, you run the risk of confirming and further entrenching exactly that conspiratorial thinking. Because that's exactly the kind of thing that 'they' would want you to think. Right?"

As Phillips indicates, all of this gets really hairy, really fast, because journalists often need to stop and talk about what does and doesn't matter, in order to keep from perpetuating even more harm. But in an age where ironic memetic rhetoric frequently distorts reality in ways that then become reality, that's extremely hard to do.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Which brings us to the New Zealand shooter's call to "subscribe to PewDiePie" right before the attack.

The call to "subscribe to PewDiePie" was the shooter's most revealing meme of all

At the most basic level, the words "subscribe to PewDiePie" are a meme. The phrase first spread as a harmless and sincere push by fans of PewDiePie, a.k.a. YouTube creator Felix Kjellberg, to get him more subscribers on the platform, specifically in response to the over-corporatization of the site. Many of those fans were so enthusiastic, however, that the campaign has since spread far beyond YouTube and his fans.

In some corners of the internet, the phrase "subscribe to PewDiePie" is used so frequently that it has essentially become meaningless, a one-line shitpost that represents a general kind of reactionary stance. Or, as the New York Times put it, "a kind of all-purpose cultural bat signal for the young and internet-absorbed." Saying "subscribe to PewDiePie" has become a way of proving that you're internet-savvy, that you're not a passive consumer of a sanitized and corporatized internet. It's a shorthand, in essence, for "us versus them."

There is currently no indication that the New Zealand shooter actually is a PewDiePie fan. And as legions of PewDiePie fans have been quick to point out in the wake of the shooting, the meme at this point has nothing to do with PewDiePie himself.

For his part, Kjellberg was quick to repudiate the attack, stating, "I feel absolutely sickened having my name uttered by this person." But for a certain audience, the statement is meant to make the shooting — which, again, was live-streamed on Facebook, with the link posted to 8chan in advance — feel normalized, as if it were just an average video game demo by the average meme-happy gamer.

And even though "subscribe to PewDiePie" is just a meme, it's not just a meme, because Kjellberg has a history of amplifying white nationalist rhetoric that is both serious and violent, and the shooter has now both drawn attention to him and used him as a messenger. "By forcing Kjellberg to acknowledge the attack," Taylor Lorenz wrote at the Atlantic, "the shooter succeeded in further spreading the word about the crime to Kjellberg's tens of millions of followers."

By drawing on meme culture, and naming a polarizing central figure within meme culture, the alleged shooter ensured that debate would arise around those details, rather than uniting people in standing against hateful rhetoric and violent acts.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

This cycle is already beginning to take effect, with many lining up to dismiss the role that memes have played in advancing far-right ideology, even though the New Zealand shooter literally described his horrific actions as an escalation of online shitposting.

The whole point of these types of memes is that they are not meant to be taken seriously, right up until the moment where they become very serious. Take it from the anonymous owner of an established anti-Semitic YouTube channel, who described his own strategy of spreading his hateful rhetoric as follows: "Pretend to joke about it until the punchline /really/ lands."

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger

By Mike Isaac | NY Times | January 25, 2019



SAN FRANCISCO — Mark Zuckerberg, Facebook's chief executive, plans to integrate the social network's messaging services — WhatsApp, Instagram and Facebook Messenger — asserting his control over the company's sprawling divisions at a time when its business has been battered by scandal.

The services will continue to operate as stand-alone apps, but their underlying technical infrastructure will be unified, said four people involved in the effort. That will bring together three of the world's largest messaging networks, which between them have more than 2.6 billion users, allowing people to communicate across the platforms for the first time.

The move has the potential to redefine how billions of people use the apps to connect with one another while strengthening Facebook's grip on users, raising antitrust, privacy and security questions. It also underscores how Mr. Zuckerberg is imposing his authority over units he once vowed to leave alone.

The plan — which is in the early stages, with a goal of completion by the end of this year or early 2020 — requires thousands of Facebook employees to reconfigure how WhatsApp, Instagram and Facebook Messenger function at their most basic levels, said the people involved in the effort, who spoke on the condition of anonymity because the matter is confidential.

Mr. Zuckerberg has also ordered that the apps all incorporate end-to-end encryption, the people said, a major step that protects messages from being viewed by anyone except the participants in a conversation.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

In a statement, Facebook said it wanted to "build the best messaging experiences we can; and people want messaging to be fast, simple, reliable and private." It added: "We're working on making more of our messaging products end-to-end encrypted and considering ways to make it easier to reach friends and family across networks."

By stitching the apps' infrastructure together, Mr. Zuckerberg hopes to increase Facebook's utility and keep users highly engaged inside the company's ecosystem. That could reduce people's appetite for rival messaging services, like those offered by Apple and Google. If users can interact more frequently with Facebook's apps, the company might also be able to increase its advertising business or add new revenue-generating services, the people said.

The change follows two years of scrutiny of Facebook's core social network, which has been criticized for allowing election meddling and the spreading of disinformation. Those and other issues have slowed Facebook's growth and damaged its reputation, raising the hackles of lawmakers and regulators around the world. Mr. Zuckerberg has repeatedly apologized for the problems and has vowed to fix them.

Knitting together Facebook's apps is a stark reversal of Mr. Zuckerberg's previous stance toward WhatsApp and Instagram, which were independent companies that Facebook acquired. At the time of the acquisitions, Mr. Zuckerberg promised WhatsApp and Instagram plenty of autonomy from their new parent company. (Facebook Messenger is a homegrown service spun off the main Facebook app in 2014.)

hatsApp and Instagram have grown tremendously since then, prompting Mr. Zuckerberg to change his thinking, one of the people said. He now believes integrating the services more tightly will benefit Facebook's entire "family of apps" in the long term by making them more useful, the person said. Mr. Zuckerberg floated the idea for months and began to promote it to employees more heavily toward the end of 2018, the people said.

The effort has caused strife within Facebook. Instagram's founders, Kevin Systrom and Mike Krieger, left the company abruptly last fall after Mr. Zuckerberg began weighing in more. WhatsApp's founders, Jan Koum and Brian Acton, departed for similar reasons. More recently, dozens of WhatsApp employees clashed with Mr. Zuckerberg over the integration plan on internal message boards and during a contentious staff meeting in December, according to four people who attended or were briefed on the event.

The integration plan raises privacy questions because of how users' data may be shared between services. WhatsApp currently requires only a phone number when new users sign up. By contrast, Facebook and Facebook Messenger ask users to provide their true identities. Matching Facebook and Instagram users to their WhatsApp handles could give pause to those who prefer to keep their use of each app separate.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



"As you would expect, there is a lot of discussion and debate as we begin the long process of figuring out all the details of how this will work," Facebook said in a statement.

Marc Rotenberg, president and executive director the Electronic Privacy Information Center, said on Friday that the change would be "a terrible outcome for internet users." He urged the Federal Trade Commission, America's de facto privacy regulator, to "act now to protect privacy and to preserve competition."

Representative Ro Khanna, Democrat of California, criticized the change on antitrust grounds.

"This is why there should have been far more scrutiny during Facebook's acquisitions of Instagram and WhatsApp, which now clearly seem like horizontal mergers that should have triggered antitrust scrutiny," he said in a message on Twitter. "Imagine how different the world would be if Facebook had to compete with Instagram and WhatsApp."

People in many countries often rely on only one or two text messaging services. In China, WeChat, which is made by Tencent, is popular, while WhatsApp is heavily used in South America. Americans are more divided in their use of such services, SMS text messages, Apple's iMessage and various Google chat apps.

For Facebook, the move also offers avenues for making money from Instagram and WhatsApp. WhatsApp currently generates little revenue; Instagram produces ad revenue but none from its messaging. Mr. Zuckerberg does not yet have specific plans for how to profit from integrating the services, said two of the people involved in the matter. A more engaged audience could result in new forms of advertising or other services for which Facebook could charge a fee, they said.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

One potential business opportunity involves Facebook Marketplace, a free Craigslist-like product where people can buy and sell goods. The service is popular in Southeast Asia and other markets outside the United States.

When the apps are knitted together, Facebook Marketplace buyers and sellers in Southeast Asia will be able to communicate with one another using WhatsApp, which is popular in the region, rather than using Facebook Messenger or another, non-Facebook text message service. That could eventually yield new ad opportunities or profit-generating services, said one of the people.

Some Facebook employees said they were confused about what made combining the messaging services so compelling to Mr. Zuckerberg. Some said it was jarring because of his past promises about independence. When Facebook acquired WhatsApp for $19 billion in 2014, Mr. Koum talked publicly about user privacy, and said, "If partnering with Facebook meant that we had to change our values, we wouldn't have done it."

Last month, during one of WhatsApp's monthly meetings for staff members, it became clear that Mr. Zuckerberg's mandate would be a priority in 2019, said a person who was there. One WhatsApp employee then conducted an analysis of how many potential new users in the United States the integration plan could bring to Facebook, said two people familiar with the study. The total was relatively meager, the analysis showed.

To assuage concerns, Mr. Zuckerberg called a follow-up meeting with WhatsApp employees a few days later, three of the people said. On Dec. 7, employees gathered around microphones at the WhatsApp offices to ask him why he was so invested in merging the services. Some said his answers were vague and meandering. Several WhatsApp employees have left or plan to leave because of Mr. Zuckerberg's plans, the people said.

Unifying the infrastructure for WhatsApp, Instagram and Facebook Messenger is technically challenging. Unlike Facebook Messenger and Instagram, WhatsApp does not store messages and keeps minimal user data. It is the only one of the services to currently use end-to-end encryption by default.

Encrypted messaging has long been supported by privacy advocates who fear governments or hackers may gain access to people's personal messages. But it will raise other issues for Facebook, particularly related to its ability to spot and curb the spread of illicit activity or disinformation.

Last year, researchers had trouble tracking disinformation on WhatsApp before the Brazilian presidential election, before eventually finding ways to do so. WhatsApp has recently placed

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

limits on how many times a message can be forwarded on the service, in an effort to reduce the distribution of false content.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FIVE COUNTRY MINISTERIAL AND JOINT MEETINGS

DAY 1: JULY 29

TIME	ITEM	LEAD
0800	**MORNING TEA**	
0815 - 0830	**Welcome and Administration** *Home Secretary welcome and theme introduction*	UK
0830 - 0915	**Ministerial statements on priorities** *Home Secretary to invite other Ministers to introduce short 'priority statements'*	ALL
0915-1000	***SESSION 1: Threat Assessment*** [redacted]	**TAB E** UK
1000 - 1015	**MORNING TEA**	
1015 - 1230	***SESSION 2: Cyber Threats*** – *Current threats and response,* [redacted] – *Cyber and 5G* – *Sessions outcomes*	**TAB 1** UK US/UK
1230 - 1330	**LUNCH: FCM Ministers +1** (No topic) **& OFFICIAL PHOTOGRAPHS**	
1330 - 1515	***SESSION 3: Emerging Technologies*** – *'Internet of Things'* – *Counter-Unmanned Aerial Systems (Drones)* – *Session outcomes*	**TAB 2** AUS UK
1515 - 1530	**AFTERNOON TEA**	
1530 - 1700	***SESSION 4: Borders & Immigration*** – – [redacted] – *Session outcomes*	**TAB 3** AUS AUS/UK
1700 - 1825	**BILATERAL/ TRILATERAL MEETINGS**	
1830 - 1900	**TRAVEL TO TOWER OF LONDON**	
1900	**JOINT FCM/ QUINTET DRINKS RECEPTION at White Tower, Tower of London**	
2000	**FCM DINNER (FCM Minister +2) in Medival Palace, Tower of London followed by Ceremony of the Keys** ***SESSION 4: Dinner Discussion: Social integration (AUS)***	**TAB 4**

s.13(1)(a)
s.15(1) - Int'l

Document Released Under the Access to Information Act / Document divulgué en vertu

FIVE COUNTRY MINISTERIAL AND JOINT MEETINGS

DAY 2: July 30

TIME	ITEM	LEAD
0900 - 1100	***SESSION 5: Industry Roundtable on CSEA*** *Attended by Microsoft, Twitter, Facebook, Google, Snap & Roblox*	TAB 5 ALL
1100 - 1115	**MORNING TEA**	
1115 - 1200	***SESSION 6: Countering Foreign Interference*** – *Election security and strengthening democracy* – *Session outcomes*	TAB 6 AUS/CAN
1200 - 1230	***SESSION 7: Draft FCM Communiqué***	TAB 7 ALL
1230 - 1315	**JOINT FCM/QUINTET LUNCH** (Ministers +1) **& OFFICIAL PHOTOGRAPHS** (FCM & Quintet Ministers Only)	
1315 - 1500	***SESSION 8: Online Harms*** – *Countering child sexual exploitation and abuse* – *Preventing terrorist use of the internet and countering extremism* – *Session outcomes*	TAB 8 UK CAN/NZ
1500 - 1515	**AFTERNOON TEA**	
1515 - 1615	***SESSION 9: Encryption*** – *Online safety* – *Session outcomes*	TAB 9 UK
1615 - 1715	***SESSSION 10: JOINT FCM/ Quintet Session — Foreign Terrorist Fighters*** – *Battlefield evidence, international justice mechanism and PNR/UNSCR 2396* – *Session outcomes*	TAB 10 UK/US
1715 - 1730	***SESSION 11: Finalise Joint Communiqué***	TAB 11 ALL
1730 - 1800	**BREAK & BILATERAL/ TRILATERAL MEETINGS**	
1815 - 1845	**PRESS CONFERENCE** (FCM Ministers Only)	
1850	**TRAVEL TO THE HONOURABLE SOCIETY OF GRAY'S INN**	
1900 - 2000	**JOINT FCM/ QUINTET DRINKS RECEPTION AT GRAY'S INN**	

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

AGENDA

TUESDAY 30 JULY 2019 – FCM and Quintet		
Time	**Event**	**Lead**
09:00 – 11:00	**Industry Roundtable on CSEA** *Attended by Microsoft, Twitter, Facebook, Google & Apple (TBC)*	ALL
11:00 – 11:15	**Morning Tea**	
11:15 – 12:00	**Countering Foreign Interference** *Election security and strengthening democracy* *Session outcomes*	AUS/CAN
12:00 – 12:30	**Agree Joint Communique**	ALL
12:30 – 13:15	**Joint Lunch – FCM Ministers and Attorneys General +1** *No discussion topic*	
13:15 – 15:00	**Joint FCM/Quintet Session: Online Harms** *Child Sexual Abuse and Explotation* *Preventing and Countering Terrorism and Violent Extremism*	**UK** **CAN/NZ**
15:00 – 15:15	**Afternoon Tea**	
15.15 – 16.15	**Joint FCM/Quintet Session: Encryption**	**UK**
16.15 – 17.15	**Joint FCM/Quintet Session: Foreign Terrorist Fighters**	**UK**
17:15 – 17:30	Joint Draft Communiqué	ALL
17:30 – 18:00	Travel to Gray's Inn	
18:00 – 21:00	**Joint Drinks Reception at Grays' Inn**	
19:00	**Attorneys General Dinner at Gray's Inn** *Bowl Food and Drinks for Officials*	

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.13(1)(a)
s.15(1) - Int'l

AGENDA

29 - 31 July 2019 at 10-11 Carlton Terrace House

Monday 29 JULY 2019 – FCM		
Time	**Event**	**Lead**
10:15 – 12:30	**Cyber Threats** *Current threats and response,* [redacted] *Cyber and 5G* *Session outcomes*	**UK** **US/UK**
17:00 - 18:30	**Bilaterals**	**NZ, US and UK**
18:30 – 19:00	Travel to Tower of London	
19:00 – 21:00	**Joint Drinks Reception at Tower of London**	

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

AGENDA

WEDNESDAY 31 JULY - Quintet		
Time	**Event**	**Lead**
9:00 – 9:10	Welcome Speech from the UK Attorney General	UK
9:10 – 10:10	**Social Media and Data Privacy Issues**	**Aus**
10:10 – 10:20	**Break**	
10:20 – 10:35	Group Photo	
10:35 – 10:50	**Signing of Statement on International Cooperation on Cybercrime** *Short speech from François Daigle, followed by a signing and photographs*	**CAN**
10:50 – 12:20	**Sentencing Frameworks**	**UK/NZ**
12:20 – 13:20	**Lunch: Attorneys General +1** *Discussion: AI in the Justice System*	
13:20 – 14:50	**Corporate Criminal Liability**	**UK**
14:50 – 15:10	**Afternoon Tea**	
15:10 – 16:25	**Hostile State Activity**	**USA**
16:25 – 16:40	Agree Communique	ALL
16:40 – 16:45	Closing remarks from the UK Attorney General	ALL
16:45 – 17:30	Press Interviews	ALL
17:30– 18:00	Travel to TBC	
18:00 – 20:00	**Close of Quintet - Informal Drinks Reception at [redacted]** ***Toast from the UK Attorney General at 19:30***	